Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
  - Acrobat Reader Invalid-ID-Handle-Error Remote Code Execution Vulnerability
  - Argosoft Mail Server Cross-Site Scripting and Script Insertion Vulnerabilities
  - Asp Press ACS Blog Access Vulnerability
  - BK Forum SQL Injection Vulnerability
  - Citrix Program Neighborhood Agent Two Vulnerabilities
  - Ecomm Professional Shopping Cart SQL Injection Vulnerability
  - Elemental Software CartWIZ SQL Injection and Cross-Site Scripting Vulnerability
  - Fastream NETFile Server File Creation Vulnerability
  - Iatek PortalApp Cross-Site Scripting Vulnerabilities
  - Magnus Lundvall Yawcam Information Disclosure Vulnerability
  - MailEnable HTTPMail Vulnerability
  - Media Online Store Portal SQL Injection Vulnerability
  - Metalinks MetaCart Multiple SQL Injection Vulnerabilities
  - Microsoft Windows Image Rendering Denial of Service Vulnerability
  - **Microsoft Exchange Server Remote Code Execution Vulnerability (Updated)**
  - Neslo Desktop Rover Denial of Service Vulnerability
  - Novell Nsure Audit Denial of Service Vulnerability
  - Ocean12 Calendar Manager SQL Injection Vulnerability
  - OneWorldStore Denial of Service Vulnerability
  - OneWorldStore Information Disclosure Vulnerability
  - Orvado ASP Nuke SQL Injection and Cross-Site Scripting Vulnerabilities
  - **PMSoftware Simple Web Server Remote Code Execution Vulnerability (Updated)**
  - PPP Infotech netMailshar Professional Two Vulnerabilities
  - RealNetworks Realplayer Enterprise Buffer Overflow Vulnerability
  - Softwin BitDefender Insecure Program Execution Vulnerability
  - Team JohnLong RaidenFTPD Information Disclosure Vulnerability
  - WheresJames Webcam Publisher Remote Code Execution Vulnerability
- UNIX / Linux Operating Systems
  - **Apple iSync mRouter Buffer Overflow**
  - **David Gay F2C Multiple Insecure Temporary File Creation (Updated)**
  - **FreeBSD Kernel 'sendfile()' Information Disclosure (Updated)**
  - GNU CPIO Directory Traversal
  - GNU GZip Directory Traversal
  - **Grip CDDB Query Buffer Overflow (Updated)**
  - HP-UX ICMP PMTUD Remote Denial of Service
  - INRIA GeneWeb Maintainer Scripts File Manipulation
  - Inter7 SQWebmail Cross-Site Scripting
  - **J. Shilling CDRTools CDRecord Insecure File Creation (Updated)**
  - JAWS Glossary Cross-Site Scripting
  - John Bradley XV Multiple Vulnerabilities
  - JunkBuster Vulnerabilities
  - KDE Kommander Remote Arbitrary Code Execution
  - LBL TCPDump Remote Denials of Service
  - **LibEXIF Library EXIF Tag Structure Validation (Updated)**
  - **LibTIFF Buffer Overflows (Updated)**
  - Red Hat logwatch secure Script Remote Denial of Service
  - **Multiple Vendors ht://Dig Cross-Site Scripting (Updated)**
  - Multiple Vendors ImageMagick Remote Buffer Overflow
  - **Multiple Vendors KDE 'kimgio' image library Remote Buffer Overflow (Updated)**
  - **Linux Kernel Multiple ISO9660 Filesystem Handling Vulnerabilities (Updated)**
  - **Multiple Vendors MySQL Database Unauthorized GRANT Privilege (Updated)**
  - **Multiple Vendors CVS Multiple Vulnerabilities (Updated)**
  - **Multiple Vendors Linux Kernel NFS I/O Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Bluetooth Signed Buffer Index (Updated)**
  - **Multiple Vendors Linux Kernel Serial Driver Mouse And Keyboard Event Injection (Updated)**
  - **Multiple Vendors Linux Kernel TmpFS Driver Local Denial of ServicE (Updated)**
  - **Multiple Vendors Linux Kernel Local Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel PPP Driver Remote Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Multiple Vulnerabilities (Updated)**
  - **Multiple Vendors Linux Kernel EXT2 File System Information Leak (Updated)**

- Multiple Vendors Linux Kernel Unw_Unwind_To_User Denial of Service
- Multiple Vendors Linux Kernel 'Fib_Seq_Start' Denial of Service
- **Multiple Vendors Linux Kernel SYS_EPoll_Wait Elevated Privileges (Updated)**
- **Multiple Vendors Linux Kernel SYSFS_Write_File Local Integer Overflow (Updated**
- **Multiple Vendors Gaim Jabber File Request Remote Denial of Service (Updated)**
- **Multiple Vendors Gaim 'Gaim_Markup_Strip_HTML()' Function Remote Denial of Service (Updated)**
- **Multiple Vendors Samba smbd Security Descriptor (Updated)**
- **Multiple Vendors XLI Internal Buffer Management (Updated)**
- **Multiple Vendors XLoadImage Compressed Image Remote Command (Updated)**
- **MySQL 'mysqlaccess.sh' Unsafe Temporary Files (Updated)**
- **OpenMosixview Multiple Insecure Temporary File Creation (Updated)**
- **PHP Group Exif Module IFD Nesting Remote Denial of Service (Updated)**
- **PHP Group Exif Module IFD Tag Integer Overflow (Updated)**
- **Remote Sensing LibTIFF Two Integer Overflow Vulnerabilities (Updated)**
- Roar Smith Info2www Cross-Site Scripting
- **Rob Flynn Gaim Multiple Remote Denials of Service (Updated)**
- SWSoft Confixx SQL Injection
- SNMPPD SNMP Proxy Daemon Remote Format String

- Multiple Operating Systems
  - Albrecht Guenther PHProjekt Chat Script Cross-Site Scripting
  - AZ Bulletin Board Multiple Vulnerabilities
  - bBlog 'postid' Cross-Site Scripting & SQL Injection
  - Castlehill Directory Traversal
  - DUportal Multiple SQL Injection
  - DUportal Pro Multiple SQL Injection
  - **eGroupWare Multiple Vulnerabilities (Updated)**
  - Ethereal RSVP Decoding Routines Denial of Service
  - FlexPHPNews News.PHP SQL Injection
  - Fritz Berger Yappa-NG Cross-Site Scripting & File Include
  - **GNU Gaim Denial of Service Vulnerability (Updated)**
  - **Gregory Demar Coppermine Photo Gallery 'include/init.inc.php' HTML Injection (Updated)**
  - Gregory Demar Coppermine Photo Gallery Multiple Vulnerabilities
  - Horde Passwd Module Parent Frame Page Title Cross-Site Scripting
  - Horde Kronolith Module Parent Frame Page Title Cross-Site Scripting
  - Horde Turba Module Parent Frame Page Title Cross-Site Scripting
  - Horde Accounts Module Parent Frame Page Title Cross-Site Scripting
  - Horde Chora Parent Frame Page Title Cross-Site Scripting
  - Horde Forwards Module Parent Frame Page Title Cross-Site Scripting
  - Horde IMP Webmail Client Parent Frame Page Title Cross-Site Scripting
  - Horde Mnemo Parent Frame Page Title Cross-Site Scripting
  - Horde Vacation Parent Frame Page Title Cross-Site Scripting
  - Horde Nag Parent Frame Page Title Cross-Site Scripting
  - IBM WebSphere Application Server Error Page Cross-Site Scripting
  - IBM iSeries AS400 FTP Service Directory Traversal
  - Intersoft NetTerm USER Remote Buffer Overflow
  - Invision Power Board 'QPid' Parameter SQL Injection
  - MediaWiki Cross-Site Scripting
  - **Mozilla Suite / Firefox Multiple Vulnerabilities (Updated)**
  - **Mozilla Suite/Firefox JavaScript Lambda Information Disclosure (Updated)**
  - MPlayer RTSP and MMST Streams Buffer Overflow
  - **Multiple Vendor TCP/IP Implementation ICMP Remote Denial of Service (Updated)**
  - MySQL MaxDB Remote Buffer Overflows
  - **MySQL CREATE FUNCTION Remote Code Execution Vulnerability (Updated)**
  - Netref 'Cat_for_gen.PHP' Remote PHP Script Injection
  - North American Systems International Bsafe Directory Traversal
  - **Oracle Database Multiple SQL Injection (Updated)**
  - Oracle Database SQL Injection & Denial of Service
  - Palace Guard Software Secure/NET+ Input Validation
  - **PHP 'getimagesize()' Multiple Denials of Service (Updated)**
  - PHP Labs proFile Cross-Site Scripting
  - PHPBB Cross-Site Scripting
  - PHPBB-Auction SQL Injection & Information Disclosure
  - PHPMyVisites Cross-Site Scripting
  - PHPMyVisites Set_Lang File Include
  - PixySoft E-Cart Input Validation
  - PowerTech PowerLock Directory Traversal
  - ProfitCode Software PayProCart Multiple Cross-Site Scripting & Path Disclosure
  - **Python SimpleXMLRPCServer Remote Code (Updated)**
  - Raz-Lee Security+++ Suite Directory Traversal
  - SafeStone Directory Traversal
  - **OpenOffice Malformed Document Remote Heap Overflow (Updated)**
  - Sun Java System Web Proxy Server Multiple Remote Buffer Overflows
  - UBBCentral UBB.threads 'Printthread.PHP' SQL Injection

- **University of California PostgreSQL Multiple Vulnerabilities (Updated)**
- VooDoo Circle BotNet Connection Remote Denial of Service
- **WebCT Discussion Board Arbitrary Code Execution (Updated)**
- WoltLab Burning Board 'PMS.PHP' Cross-Site Scripting
- WoltLab Burning Board 'Thread.PHP' Cross-Site Scripting

Recent Exploit Scripts/Techniques
Trends
Viruses/Trojans

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Adobe Acrobat Reader 6.0 and prior	A vulnerability has been reported that could let a remote malicious user execute arbitrary code. If a specially crafted PDF file is loaded by Acrobat Reader it will trigger an Invalid-ID-Handle-Error in 'AcroRd32.exe'. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Acrobat Reader Invalid-ID-Handle-Error Remote Code Execution Vulnerability	High	Security Tracker Alert ID: 1013774, April 21, 2005
Argosoft.com ArGoSoft Mail Server 1.8.7.6	Two vulnerabilities have been reported that could let remote malicious users conduct Cross-Site Scripting and script insertion attacks. This is due to input validation errors in parameters passed to mails and user settings. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Argosoft Mail Server Cross-Site Scripting and Script Insertion Vulnerabilities CAN-2005-1282	High	Secunia SA15100, April 26, 2005
Asp Press ACS Blog 1.1.3 and prior	An authentication vulnerability was reported that could let a remote malicious user gain administrative privileges on the application. The 'inc_login_check.asp' script grants administrative privileges to the remote user if a certain cookie is set. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Asp Press ACS Blog Access Vulnerability CAN-2005-1288	Medium	Security Tracker Alert ID, 1013795, April 25, 2005
Black Knight Development BK Forum 4	An input validation vulnerability has been reported that could let a remote malicious user inject SQL commands. Several scripts do not properly validate user-supplied input. A remote user can create parameter values to execute SQL commands on the underlying database. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	BK Forum SQL Injection Vulnerability CAN-2005-1287	High	Security Tracker Alert ID, 1013793, April 25, 2005
Citrix Program Neighborhood Agent for Win32 Citrix MetaFrame	Buffer overflow and unspecified vulnerabilities have been reported that could let remote malicious users execute arbitrary code or create arbitrary shortcuts. Update to: * Program Neighborhood Agent for Win32 versions 9.0 and later. * Citrix MetaFrame Presentation Server client for WinCE versions 8.33	Citrix Program Neighborhood Agent Two Vulnerabilities CAN-2004-1077 CAN-2004-1078	High	Citrix Document ID: CTX105650, April 25, 2005

Presentation Server client for WinCE (versions including Program Neighborhood Agent)	and later. Available at: http://www.citrix.com/English/SS/downloads/downloads.asp?dID=2755 A Proof of Concept exploit has been published.			
Ecommerce-Carts.com Ecomm Professional Shopping Cart 3	A vulnerability has been reported which can be exploited by remote malicious users to conduct SQL injection attacks. Input passed to the 'AdminPWD' parameter in 'verify.asp' isn't properly verified before used in an SQL query. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Ecomm Professional Shopping Cart SQL Injection Vulnerability	High	IHS Iran Hackers Sabotage Public advisory, April 19, 2005
Elemental Software CartWIZ	Several vulnerabilities have been reported that could let a remote malicious user inject SQL commands and conduct Cross-Site Scripting attacks. Several scripts do not properly validate user-supplied input. A remote user can create parameter values that will execute SQL commands on the underlying database. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Elemental Software CartWIZ SQL Injection and Cross-Site Scripting Vulnerability CAN-2005-1291 CAN-2005-1292	High	Security Tracker Alert ID, 1013792, April 25, 2005
Fastream Technologies NETFile Server prior to 7.5.0 Beta 7; Tested on 7.4.6 on English Win2K SP4	A vulnerability has been reported that could let a remote authenticated malicious user upload or delete files or directories located outside of the FTP directory. A fixed version (7.5.0 Beta 7) is available: http://ww.fastream.com/products.htm A Proof of Concept exploit has been published.	Fastream NETFile Server File Creation Vulnerability	Medium	SIG^2 Vulnerability Research, April 25, 2005
Iatek PortalApp 3.3	Input validation vulnerabilities have been reported that could let a remote user conduct Cross-Site Scripting attacks. The 'ContentId,' 'CatId,' 'ContentTypeId,' and 'ForumId' parameters are not properly filtered to remove HTML code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Iatek PortalApp Cross-Site Scripting Vulnerabilities	High	Security Tracker Alert ID, 1013755, April 19, 2005
Magnus Lundvall Yawcam 0.2.5	A vulnerability has been reported that could let a remote malicious user obtain files on the target system that are located outside of the web document directory. This is because the web service does not properly validate user-supplied HTTP GET requests. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Magnus Lundvall Yawcam Information Disclosure Vulnerability CAN-2005-1230	Medium	Security Tracker Alert ID, 1013781, April 21, 2005
MailEnable MailEnable	A potential "security exploit" vulnerability with an unknown impact has been reported by the vendor. The vendor has issued a fix: http://www.mailenable.com/hotfix/MEHTTPS.zip Currently we are not aware of any exploits for this vulnerability.	MailEnable HTTPMail Vulnerability	Not Specified	Security Tracker Alert ID, 1013786, April 22, 2005
Media Online Italia Store Portal 2.63	A vulnerability has been reported that could let a remote malicious user inject SQL commands. Several scripts do not properly validate user-supplied input in various parameters when processed as a Referrer URL. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Media Online Store Portal SQL Injection Vulnerability CAN-2005-1293	High	Dcrab 's Security Advisory, April 24, 2005
MetaLinks MetaCart and MetaCart2	Multiple input validation vulnerabilities have been reported that could let malicious users inject SQL commands. These vulnerabilities may lead to theft of sensitive information, potentially including authentication credentials, and data corruption. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Metalinks MetaCart Multiple SQL Injection Vulnerabilities	High	Security Focus, Bugtraq ID 13377, 13382, 13383, 13384, 13385, 13376, 13393, April 26, 2005
Microsoft Windows XP Home Edition and Professional Edition	A vulnerability has been reported that could let a user cause a Denial of Service. This is due to an error in the image rendering for overly large images. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Image Rendering Denial of Service Vulnerability	Low	Secunia SA15064, April 22, 2005

Microsoft Exchange 2000 Server SP3, 2003, 2003 SP1	A vulnerability has been reported due to an unchecked buffer in the SMTP service that could let a remote malicious user execute arbitrary code. V1.1: Bulletin updated to reflect a revised "Security Update Information" section for the Word 2003 security update. Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-021.mspx **A Proof of Concept exploit script has been published.**	Microsoft Exchange Server Remote Code Execution Vulnerability CAN-2005-0560	High	Microsoft Security Bulletin. MS05-021, April 12, 2005 Technical Cyber Security Alert TA05-102A US CERT VU#275193 Microsoft Security Bulletin. MS05-021 V1.1, April 14, 2005 **Security Focus, 13118, April 20, 2005**
Neslo Desktop Rover 3.0	A vulnerability has been reported which could let a local malicious user cause a Denial of Service. This is due to an error in the communication handling on port 61427/tcp. Update to upcoming 3.1 version. A Proof of Concept exploit has been published.	Neslo Desktop Rover Denial of Service Vulnerability CAN-2005-1204	Low	Evil Packet Advisory EP-000-0003, April 19, 2005
Novell Novell Nsure Audit 1.01	A vulnerability has been reported in the processing of ASN.1 messages that could let a remote malicious user cause Denial of Service conditions. A brute force attack against 'webadmin.exe' will cause a Denial of Service. Update to version 1.0.3. A Proof of Concept exploit has been published.	Novell Nsure Audit Denial of Service Vulnerability CAN-2005-1247	Low	Novell Technical Information Document, TID10097379, April 19, 2005
Ocean12 Ocean 12 Calendar 1.01	A vulnerability has been reported that could let a remote malicious user inject SQL commands. This is due to input validation errors in the 'Admin_password' field. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Ocean12 Calendar Manager SQL Injection Vulnerability CAN-2005-1223	High	Hackers Center Security Group, Zinho's Security Advisory, April 19, 2005
OneWorldStore OneWorldStore	A vulnerability has been reported that could let a remote malicious user cause a Denial of Service condition. A remote user can directly access the '/owConnections/chksettings.asp' file to cause the application to crash. Fix available at: http://www.oneworldstore.com/support_security_issue_updates.asp#April_20_2005_Lostmon A Proof of Concept exploit has been published.	OneWorldStore Denial of Service Vulnerability CAN-2005-1328	Low	Security Tracker Alert ID,: 1013782, April 22, 2005
OneWorldStore OneWorldStore	An information disclosure vulnerability has been reported that could let a remote malicious user view order information. A remote user can execute the 'PaymentMethods/owOfflineCC.asp' script with a unique 'idOrder' value to obtain information about another user's order. A fix is available at: http://oneworldstore.com/support_updates.asp A Proof of Concept exploit has been published.	OneWorldStore Information Disclosure Vulnerability CAN-2005-1329	Medium	Security Tracker Alert ID, 1013796, April 25, 2005
Orvado Technologies ASP Nuke 0.80	Several vulnerabilities have been reported that could let a remote malicious user inject SQL commands or conduct Cross-Site Scripting attacks. The 'profile.asp' and 'select.asp' scripts do not filter HTML code from user-supplied input before displaying the information. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Orvado ASP Nuke SQL Injection and Cross-Site Scripting Vulnerabilities	High	Dcrab Security Advisory, April 22, 2005
PMSoftware Simple Web Server 1.0.15	A buffer overflow vulnerability has been reported that could let a remote malicious user cause a Denial of Service or execute arbitrary code. No workaround or patch available at time of publishing. **Exploit scripts have been published.**	PMSoftware Simple Web Server Remote Code Execution Vulnerability CAN-2005-1173	Low/ High (High if arbitrary code can be executed)	Secunia SA15000, April 19, 2005 **Security Focus, 13227, April 20, 2005**
PPP Infotech netMailshar Professional 4.0 build 15	Multiple vulnerabilities have been reported that could disclose sensitive information and valid user accounts. These is because of an input validation error in the Webmail service (port 8003) and because the Webmail service returns different error messages if a certain username is valid or not. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	PPP Infotech netMailshar Professional Two Vulnerabilities	Medium	Secunia SA15038, April 21, 2005
RealNetworks RealPlayer Enterprise 1.1, 1.2, 1.5, 1.6, and 1.7	A vulnerability has been reported that could let a remote malicious user execute arbitrary code. This is due to a boundary error in 'pnen3260.dll' when processing RAM files that can be exploited to cause a buffer overflow. An updated versions of pnen3260.dll is available:	RealNetworks Realplayer Enterprise Buffer Overflow Vulnerability	High	Security Patch Update For Realplayer Enterprise, April 19, 2005

	http://docs.real.com/docs/pnen3260.dll Currently we are not aware of any exploits for this vulnerability.	CAN-2005-0755		
Softwin BitDefender Antivirus Standard 8.x, BitDefender Antivirus Professional Plus 8.x	A vulnerability has been reported that could let local malicious users disable the virus protection or gain escalated privileges.This is because the installation process can create entries insecurely in the 'Run' registry key to automatically run some programs when a user logs in. The vendor recommends quoting the command line of the created entries in the registry. A Proof of Concept exploit has been published.	Softwin BitDefender Insecure Program Execution Vulnerability CAN-2005-1286	High	Secunia SA15076, April 26, 2005
Team JohnLong RaidenFTPD 2.x	A vulnerability has been reported which can be exploited by remote malicious users to gain knowledge of sensitive information. It is possible to access arbitrary files outside the FTP root. Update to version 2.4 build 2241: http://www.raidenftpd.com/en/download.html Currently we are not aware of any exploits for this vulnerability.	Team JohnLong RaidenFTPD Information Disclosure Vulnerability	Medium	Raiden Professional bulletin board advisory, April 20, 2005
Where's James Software WheresJames Webcam Publisher Beta 2.0.0014	A buffer overflow vulnerability exists that could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	WheresJames Webcam Publisher Remote Code Execution Vulnerability	High	Security Tracker Alert ID,: 1013757, April 19, 2005

back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Apple Mac OS X 10.3.7 with iSync	A buffer overflow vulnerability exists in 'mRouter' when specially crafted options to the '-v' and '-a' command line switches are submitted, which could let a malicious user obtain root privileges. **Upgrade available at:** **http://www.apple.com/support/downloads/securityupdate2005004.html** An exploit script has been published.	Apple iSync mRouter Buffer Overflow CAN-2005-0193	High	Securiteam, January 23, 2005 **Apple Security Update, APPLE-SA-2005-04-19, April 19, 2005**
David M. Gay f2c Fortran 77 Translator 1.3.1	Several vulnerabilities exist due to the insecure creation of temporary files, which could let a malicious user modify information or obtain elevated privileges. **Debian:** **http://security.debian.org/pool/updates/main/f/f2c/** Gentoo: http://security.gentoo.org/glsa/glsa-200501-43.xml There is no exploit required.	F2C Multiple Insecure Temporary File Creation CVE Names: CAN-2005-0017 CAN-2005-0018	Medium	Debian Security Advisory, DSA 661-1, January 27, 2005 Gentoo Linux Security Advisory GLSA 200501-43, January 30, 2005 **Debian Security Advisory, DSA 661-2, April 20,2005**
FreeBSD FreeBSD 5.4 & prior	A vulnerability has been reported in the 'sendfile()' system call due to a failure to secure sensitive memory before distributing it over the network, which could let a malicious user obtain sensitive information. Patches available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:02/ There is no exploit code required.	FreeBSD Kernel 'sendfile()' Information Disclosure CAN-2005-0708	Medium	FreeBSD Security Advisory, FreeBSD-SA-05:02, April 5, 2005 **US-CERT VU#604846**
GNU cpio 2.6	A Directory Traversal vulnerability has been reported when invoking cpio on a malicious archive, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	CPIO Directory Traversal CAN-2005-1229	Medium	Bugtraq, 396429, April 20, 2005
GNU gzip 1.2.4 a, 1.2.4, 1.3.3-1.3.5	A Directory Traversal vulnerability has been reported due to an input validation error when using 'gunzip' to extract a file with the '-N' flag, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GNU GZip Directory Traversal CAN-2005-1228	Medium	Bugtraq, 396397, April 20, 2005

Grip Grip 3.1.2, 3.2 .0	A buffer overflow vulnerability has been reported in the CDDB protocol due to a boundary error, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://security.gentoo.org/glsa/glsa-200503-21.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-304.html Mandrake: http://www.mandrakesecure.net/en/ftp.php Gentoo: http://security.gentoo.org/glsa/glsa-200504-07.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **Peachtree:** **http://peachtree.burdell.org/updates/** Currently we are not aware of any exploits for this vulnerability.	Grip CDDB Query Buffer Overflow CAN-2005-0706	Low/ High (High if arbitrary code can be executed)	Fedora Update Notifications, FEDORA-2005-202 & 203, March 9, 2005 Gentoo Linux Security Advisory, GLSA 200503-21, March 17, 2005 RedHat Security Advisory, RHSA-2005:304-08, March 28, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:066, April 3, 2005 Gentoo Linux Security Advisory, GLSA 200504-07, April 8, 2005 SUSE Security Summary Report, SUSE-SR:2005:010, April 8, 2005 **Mandriva Linux Security Update Advisories, MDKSA-2005:074 & 075, April 21, 2005** **Peachtree Linux Security Notice, PLSN-0007, April 22, 2005**
Hewlett Packard Company HP-UX B.11.23, B.11.22, B.11.11, B.11.04, B.11.00	A remote Denial of Service vulnerability has been reported in the Path MTU Discovery (PMTUD) functionality that is supported in the ICMP protocol. Patches available at: http://www1.itrc.hp.com/service/cki/docDisplay.do?docId= HPSBUX01137 Currently we are not aware of any exploits for this vulnerability.	HP-UX ICMP PMTUD Remote Denial of Service CAN-2005-1192	Low	Hewlett Packard Company Security Advisory, HPSBUX01137, April 24, 2005
INRIA GeneWeb 4.0 5-4.0 9	A vulnerability has been reported in the maintainer scripts because files believed to be old '.gwb' datafile files are converted automatically without checking file permissions and content, which could let a malicious user modify arbitrary files. Debian: http://security.debian.org/pool/updates/main/g/geneweb/ Currently we are not aware of any exploits for this vulnerability.	INRIA GeneWeb Maintainer Scripts File Manipulation CAN-2005-0391	Medium	Debian Security Advisory, DSA 712-1 , April 19, 2005
Inter7 SqWebMail 3.4.1, 3.5 .0-3.5.3, 3.6.0-3.6.1, 4.0.4.20040524, 4.0.5.	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of the 'redirect' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Inter7 SQWebmail Cross-Site Scripting CAN-2005-1308	High	Security Focus, 13374, April 26, 2005
J. Schilling CDRTools 2.0	A vulnerability has been reported in cdrecord due to insecure creation of various files, which could let a malicious user corrupt arbitrary files. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/cdrtools/ **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** There is no exploit code required.	CDRTools CDRecord Insecure File Creation CAN-2005-0866	Medium	Ubuntu Security Notice USN-100-1, March 24, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:077, April 21, 2005**

JAWS JAWS 0.3-0.5 beta2	A Cross-Site Scripting vulnerability has been reported in the Glossary module due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	JAWS Glossary Cross-Site Scripting CAN-2005-1231	High	Securiteam, April 21, 2005
John Bradley XV 3.10 a	Multiple vulnerabilities have been reported:a buffer overflow vulnerability was reported in the PDS image decoder when processing comments, which could let a remote malicious user execute arbitrary code; a vulnerability was reported in the TIFF and PDS image decoders due to format string errors, which could let a remote malicious execute arbitrary code; a vulnerability was reported due to an input validation error when handling filenames, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200504-17.xml There is no exploit code required.	John Bradley XV Multiple Vulnerabilities	High	Secunia Advisory, SA14977, April 19, 2005 Gentoo Linux Security Advisory, GLSA 200504-17, April 19, 2005
Junkbuster Internet Junkbuster 2.0.1, 2.0.2	Two vulnerabilities have been reported: a vulnerability has been reported in the 'ij_untrusted_url()' function, which could let a remote malicious user modify the configuration; and a vulnerability has been reported due to errors when filtering URLs, which could let a malicious user cause a Denial of Service or execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200504-11.xml Debian: http://security.debian.org/pool/updates/main/j/junkbuster/ Currently we are not aware of any exploits for these vulnerabilities.	JunkBuster Vulnerabilities CAN-2005-1108 CAN-2005-1109	Low/ High (High if arbitrary code can be executed)	Gentoo Linux Security Advisory GLSA 200504-11, April 13, 2005 **Debian Security Advisory, DSA 713-1, April 21, 2005**
KDE KDE 3.2-3.2.3, 3.3-3.3.2, 3.4, KDE Quanta 3.1	A vulnerability has been reported due to a design error in Kommander, which could let a remote malicious user execute arbitrary code. Patches available at: ftp://ftp.kde.org/pub/kde/security_patches/f Gentoo: http://security.gentoo.org/glsa/glsa-200504-23.xml Currently we are not aware of any exploits for this vulnerability.	KDE Kommander Remote Arbitrary Code Execution CAN-2005-0754	High	KDE Security Advisory, April 20, 2005 Gentoo Linux Security Advisory, GLSA 200504-23, April 22, 2005
LBL tcpdump 3.4 a6, 3.4, 3.5, alpha, 3.5.2, 3.6.2, 3.6.3, 3.7-3.7.2, 3.8.1 -3.8.3	Remote Denials of Service vulnerabilities have been reported due to the way tcpdump decodes Border Gateway Protocol (BGP) packets, Label Distribution Protocol (LDP) datagrams, Resource ReSerVation Protocol (RSVP) packets, and Intermediate System to Intermediate System (ISIS) packets. No workaround or patch available at time of publishing. Exploit scripts have been published.	LBL TCPDump Remote Denials of Service CAN-2005-1278 CAN-2005-1279 CAN-2005-1280	Low	Bugtraq, 396932, April 26, 2005

libexif libexif 0.6.9, 0.6.11	A vulnerability exists in the 'EXIF' library due to insufficient validation of 'EXIF' tag structure, which could let a remote malicious user execute arbitrary code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libe/libexif/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-17.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-300.html Mandrake: http://www.mandrakesecure.net/en/ftp.php Debian: http://security.debian.org/pool/updates/main/libe/libexif/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **Peachtree:** **http://peachtree.burdell.org/updates/** Currently we are not aware of any exploits for this vulnerability.	LibEXIF Library EXIF Tag Structure Validation CAN-2005-0664	High	Ubuntu Security Notice USN-91-1, March 7, 2005 Fedora Update Notifications, FEDORA-2005-199 & 200, March 8, 2005 Gentoo Linux Security Advisory, GLSA 200503-17, March 12, 2005 RedHat Security Advisory, RHSA-2005:300-08, March 21, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:064, March 31, 2005 Debian Security Advisory, DSA 709-1, April 15, 2005 SUSE Security Summary Report, SUSE-SR:2005:011, April 15, 2005 **Peachtree Linux Security Notice, PLSN-0006, April 22, 2005**
libtiff.org LibTIFF 3.6.1 Avaya MN100 (All versions), Avaya Intuity LX (version 1.1-5.x), Avaya Modular Messaging MSS (All versions)	Several buffer overflow vulnerabilities exist: a vulnerability exists because a specially crafted image file can be created, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a remote Denial of Service vulnerability exists in 'libtiff/tif_dirread.c' due to a division by zero error; and a vulnerability exists in the 'tif_next.c,' 'tif_thunder.c,' and 'tif_luv.c' RLE decoding routines, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/t/tiff/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-11.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ OpenPKG: ftp://ftp.openpkg.org/release/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-577.html Slackware: ftp://ftp.slackware.com/pub/slackware/ Conectiva: ftp://atualizacoes.conectiva.com.br/ KDE: Update to version 3.3.2: http://kde.org/download/ Apple Mac OS X:	LibTIFF Buffer Overflows CAN-2004-0803 CAN-2004-0804 CAN-2004-0886	Low/ High (High if arbitrary code can be execute)	Gentoo Linux Security Advisory, GLSA 200410-11, October 13, 2004 Fedora Update Notification, FEDORA-2004-334, October 14, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.043, October 14, 2004 Debian Security Advisory, DSA 567-1, October 15, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:109 & MDKSA-2004:111, October 20 & 21, 2004 SuSE Security Announcement, SUSE-SA:2004:038, October 22, 2004 RedHat Security Advisory, RHSA-2004:577-16, October 22, 2004 Slackware Security Advisory, SSA:2004-305-02, November 1, 2004 Conectiva Linux Security Announcement, CLA-2004:888, November 8, 2004 US-CERT Vulnerability Notes

	http://www.apple.com/swupdates/ Gentoo: KDE kfax: http://www.gentoo.org/security/en/glsa/glsa-200412-17.xml Avaya: No solution but workarounds available at: http://support.avaya.com/elmodocs2/security/ASA-2005-002_RHSA-2004-577.pdf TurboLinux: http://www.turbolinux.com/update/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-354.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.19 RedHat: http://rhn.redhat.com/errata/RHSA-2005-021.html **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** **Sun:** **http://sunsolve.sun.com/search/document.do?assetkey=1-26-57769-1** Proofs of Concept exploits have been published.			VU#687568 & VU#948752, December 1, 2004 Gentoo Linux Security Advisory, GLSA 200412-02, December 6, 2004 KDE Security Advisory, December 9, 2004 Apple Security Update SA-2004-12-02 Gentoo Security Advisory, GLSA 200412-17 / kfax, December 19, 2004 Avaya Advisory ASA-2005-002, January 5, 2005 Conectiva Linux Security Announcement, CLA-2005:914, January 6, 2005 Turbolinux Security Announcement, January 20, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:052, March 4, 2005 RedHat Security Advisory, RHSA-2005:354-03, April 1, 2005 RedHat Security Advisory, RHSA-2005:021-09, **SGI Security Advisory, 20050404-01-U, April 20, 2005** **Sun(sm) Alert Notification, 57769, April 25, 2005**
LogWatch LogWatch 2.1.1, 2.5, 2.6	A remote Denial of Service vulnerability has been reported in the logwatch secure script due to a parsing error. RedHat: http://rhn.redhat.com/errata/RHSA-2005-364.html There is no exploit code required; however, a Proof of Concept exploit has been published.	Red Hat logwatch secure Script Remote Denial of Service CAN-2005-1061	Low	GulfTech Security Research, April 19, 2005
Multiple Vendors ht//Dig Group ht://Dig 3.1.5 -8, 3.1.5 -7, 3.1.5, 3.1.6, 3.2 .0, 3.2 0b2-0b6; SuSE Linux 8.0, i386, 8.1, 8.2, 9.0, 9.0 x86_64, 9.1, 9.2	A Cross-Site Scripting vulnerability exists due to insufficient filtering of HTML code from the 'config' parameter, which could let a remote malicious user execute arbitrary HTML and script code. SuSE: ftp://ftp.suse.com/pub/suse/ Debian: http://security.debian.org/pool/updates/main/h/htdig/ Gentoo: http://security.gentoo.org/glsa/glsa-200502-16.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** Proof of Concept exploit has been published.	ht://Dig Cross-Site Scripting CVE Name: CAN-2005-0085	High	SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 Debian Security Advisory ,DSA 680-1, February 14, 2005 Gentoo Linux Security Advisory, GLSA 200502-16, February 14, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:063, March 31, 2005 **Fedora Update Notification, FEDORA-2005-367, April 19, 2005**

Multiple Vendors ImageMagick 6.0-6.0.8, 6.1-6.1.8, 6.2 .0.7, 6.2 .0.4, 6.2, 6.2.1	A buffer overflow vulnerability has been reported due to a failure to properly validate user-supplied string lengths before copying into static process buffers, which could let a remote malicious user cause a Denial of Service. Upgrades available at: http://www.imagemagick.org/script/binary-releases.php A Proof of Concept exploit has been published.	ImageMagick Remote Buffer Overflow CAN-2005-1275	Low	Security Focus, 13351, April 25, 2005
Multiple Vendors KDE 2.0, beta, 2.0.1, 2.1-2.1.2, 2.2-2.2.2, 3.0-3.0.5, 3.1-3.1.5, 3.2-3.2.3, 3.3-3.3.2, 3.4; Novell Linux Desktop 9; SuSE E. Linux 9.1, x86_64, 9.2, x86_64, 9.3, Linux Enterprise Server 9	A buffer overflow vulnerability has been reported in the 'kimgio' image library due to insufficient validation of PCX image data, which could let a remote malicious user cause a Denial of Service or possibly execute arbitrary code. Patches available at: http://bugs.kde.org/attachment.cgi?id=10325&action=view http://bugs.kde.org/attachment.cgi?id=10326&action=view SuSE: ftp://ftp.suse.com/pub/suse/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200504-22.xml** **Debian:** **http://security.debian.org/pool/updates/main/k/kdelibs/** Denial of Service Proofs of Concept exploits have been published.	KDE 'kimgio' image library Remote Buffer Overflow CAN-2005-1046	Low/ High (High if arbitrary code can be executed)	SUSE Security Announcement, SUSE-SA:2005:022, April 11, 2005 **Gentoo Linux Security Advisory, GLSA 200504-22, April 22, 2005** **Debian Security Advisory, DSA 714-1, April 26, 2005**
Multiple Vendors Linux kernel 2.4 .0-test1-test12, 2.4-2.4.29, 2.6, 2.6-test1-test11, 2.6.1-2.6.11	Multiple vulnerabilities have been reported in the ISO9660 handling routines, which could let a malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-366.html** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Multiple ISO9660 Filesystem Handling Vulnerabilities CAN-2005-0815	High	Security Focus, 12837, March 18, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Ubuntu Security Notice, USN-103-1, April 1, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 **RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005**
Multiple Vendors MySQL AB MySQL 3.20 .x, 3.20.32 a, 3.21.x, 3.22 .x, 3.22.26-3.22.30, 3.22.32, 3.23 .x, 3.23.2-3.23.5, 3.23.8-3.23.10, 3.23.22-3.23.34, 3.23.36-3.23.54, 3.23.56, 3.23.58, 3.23.59, 4.0.0-4.0.15, 4.0.18, 4.0.20; Trustix Secure Enterprise Linux 2.0, Secure Linux 1.5, 2.0, 2.1	A vulnerability exists in the 'GRANT' command due to a failure to ensure sufficient privileges, which could let a malicious user obtain unauthorized access. Upgrades available at: http://dev.mysql.com/downloads/mysql/4.0.html OpenPKG: ftp.openpkg.org RedHat: http://rhn.redhat.com/errata/RHSA-2004-611.html SuSE: ftp://ftp.suse.com/pub/suse Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/m Fedora: http://download.fedora.	MySQL Database Unauthorized GRANT Privilege CAN-2004-0957	Medium	Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 Fedora Update Notification, FEDORA-2004-530, December 8, 2004 Turbolinux Security Announcement, February 17, 2005 Fedora Legacy Update Advisory, FLSA:2129, March 24, 2005 Ubuntu Security Notice, USN-109-1 April 06, 2005 Debian Security Advisory, DSA 707-1, April 13, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:070, April 13, 2005

	redhat.com/pub/fedora/linux/core/updates/2/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ FedoraLegacy: http://download.fedoralegacy.org/fedora/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/ Debian: http://security.debian.org/pool/updates/main/m/mysql/ Mandrake: http://www.mandrakesecure.net/en/ftp.php **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** There is no exploit code required.			**Conectiva Linux Security Announcement, CLA-2005:947, April 20, 2005**
Multiple Vendors Concurrent Versions System (CVS) 1.x;Gentoo Linux; SuSE Linux 8.2, 9.0, 9.1, x86_64, 9.2, x86_64, 9.3, Linux Enterprise Server 9, 8, Open-Enterprise-Server 9.0, School-Server 1.0, SUSE CORE 9 for x86, UnitedLinux 1.0	Multiple vulnerabilities have been reported: a buffer overflow vulnerability was reported due to an unspecified boundary error, which could let a remote malicious user potentially execute arbitrary code; a remote Denial of Service vulnerability was reported due to memory leaks and NULL pointer dereferences; an unspecified error was reported due to an arbitrary free (the impact was not specified), and several errors were reported in the contributed Perl scripts, which could let a remote malicious user execute arbitrary code. Update available at: https://ccvs.cvshome.org/servlets/ProjectDocumentList **Gentoo:** **http://security.gentoo.org/glsa/glsa-200504-16.xml** SuSE: ftp://ftp.suse.com/pub/suse/i **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **Trustix:** **http://http.trustix.org/pub/trustix/updates/** **FreeBSD:** **ftp://ftp.FreeBSD.org/pub/** **Peachtree:** **http://peachtree.burdell.org/updates/** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-387.html** Currently we are not aware of any exploits for these vulnerabilities.	CVS Multiple Vulnerabilities CAN-2005-0753	Low/ High (High if arbitrary code can be executed)	Gentoo Linux Security Advisory, GLSA 200504-16, April 18, 2005 SuSE Security Announcement, SUSE-SA:2005:024, April 18, 2005 Secunia Advisory, SA14976, April 19, 2005 **Fedora Update Notification, FEDORA-2005-330, April 20, 2006** **Mandriva Linux Security Update Advisory, MDKSA-2005:073, April 21, 2005** **Trustix Secure Linux Security Advisory, TSLSA-2005-0013, April 21, 2005** **Gentoo Linux Security Advisory [UPDATE], GLSA 200504-16:02, April 22, 2005** **FreeBSD Security Advisory, FreeBSD-SA-05:05, April 22, 2005** **Peachtree Linux Security Notice, PLSN-0005, April 22, 2005** **RedHat Security Advisory, RHSA-2005:387-06, April 25, 2005**
Multiple Vendors Linux kernel 2.4 .0-test1-test12, 2.4-2.4.28, 2.4.29rc1&rc2, 2.5 .0-2.5.69, 2.6 -test1-test11, 2.6-2.6.10; SuSE . Linux 8.1, 8.2, 9.0	A Denial of Service vulnerability exists with Direct I/O access to NFS file systems. SuSE: ftp://ftp.suse.com/pub/suse/ Conectiva: ftp://atualizacoes.conectiva.com.br/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-366.html**	Linux Kernel NFS I/O Denial of Service CAN-2005-0207	Low	SUSE Security Announcement, SUSE-SA:2005:003, January 21, 2005 Conectiva Linux Security Announcement, CLA-2005:930, March 7, 2005 **RedHat Security Advisory, RHSA-2005:366-19, April**

	Currently we are not aware of any exploits for this vulnerability.			**19, 2005**
Multiple Vendors Linux kernel 2.4-2.4.29, 2.6 .10, 2.6-2.6.11	A vulnerability has been reported in the 'bluez_sock_create()' function when a negative integer value is submitted, which could let a malicious user execute arbitrary code with root privileges. Patches available at: http://www.kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.30-rc3.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-366.html** A Proof of Concept exploit script has been published.	Linux Kernel Bluetooth Signed Buffer Index CAN-2005-0750	High	Security Tracker Alert, 1013567, March 27, 2005 SUSE Security Announcement, SUSE-SA:2005:021, April 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0011, April 5, 2005 US-CERT VU#685461 Fedora Update Notification FEDORA-2005-313, April 11, 2005 **RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005**
Multiple Vendors Linux kernel 2.4-2.4.30, 2.6-2.6.11	A vulnerability has been reported due to insufficient access control of the 'N_MOUSE' line discipline, which could let a malicious user inject mouse and keyboard events into an alternate X session or console. Patches available at: http://www.securityfocus.com/data/vulnerabilities/patches/serport.patch Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-366.html** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Serial Driver Mouse And Keyboard Event Injection CAN-2005-0839	Medium	Security Focus, 12971, April 1, 2005 **RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005**
Multiple Vendors Linux kernel 2.4-2.4.30, 2.6-2.6.11; Ubuntu Linux 4.1 ppc, ia64, ia32	A Denial of Service vulnerability has been reported in the 'TmpFS' driver due to insufficient sanitization of the 'shm_nopage()' argument. Patch available at: http://www.securityfocus.com/data/vulnerabilities/patches/shmem.patch Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-366.html** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel TmpFS Driver Local Denial of Service CAN-2005-0977	Low	Security Focus, 12970 April 1, 2005 **RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005**
Multiple Vendors Linux Kernel 2.6.10, 2.6 -test1-test11, 2.6-2.6.11	A Denial of Service vulnerability has been reported in the 'load_elf_library' function. Patches available at: http://www.kernel.org/pub/linux/kernel/v2.6/patch-2.6.11.6.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **RedHat:**	Linux Kernel Local Denial of Service CAN-2005-0749	Low	Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0011, April 5, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 **RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005**

	http://rhn.redhat.com/errata/RHSA-2005-366.html Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors Linux kernel 2.6.10, 2.6 -test9-CVS, 2.6 -test1-test11, 2.6, 2.6.1 rc1&rc2, 2.6.1-2.6.8	A remote Denial of Service vulnerability has been reported in the Point-to-Point Protocol (PPP) Driver. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ Trustix: http://http.trustix.org/pub/trustix/updates SUSE: ftp://ftp.SUSE.com/pub/SUSE Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-366.html** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel PPP Driver Remote Denial of Service CAN-2005-0384	Low	Ubuntu Security Notice, USN-95-1 March 15, 2005 Trustix Secure Linux Security Advisory, TSL-2005-0009, March 21, 2005 SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 ALTLinux Security Advisory, March 29, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 **RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005**
Multiple Vendors Linux kernel 2.6.10, 2.6 -test9-CVS, 2.6-test1- -test11, 2.6, 2.6.1-2.6.11 ; RedHat Desktop 4.0, Enterprise Linux WS 4, ES 4, AS 4	Multiple vulnerabilities exist: a vulnerability exists in the 'shmctl' function, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists in 'nls_ascii.c' due to the use of incorrect table sizes; a race condition vulnerability exists in the 'setsid()' function; and a vulnerability exists in the OUTS instruction on the AMD64 and Intel EM64T architecture, which could let a malicious user obtain elevated privileges. RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ Conectiva: ftp://atualizacoes.conectiva.com.br/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-366.html** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Multiple Vulnerabilities CAN-2005-0176 CAN-2005-0177 CAN-2005-0178 CAN-2005-0204	Low/ Medium (Low if a DoS)	Ubuntu Security Notice, USN-82-1, February 15, 2005 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Conectiva Linux Security Announcement, CLA-2005:945, March 31, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 **RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005**

Multiple Vendors Linux kernel 2.6.10, 2.6, -test1-test 11, 2.6.1- 2.6.11; RedHat Fedora Core2	A vulnerability has been reported in the EXT2 filesystem handling code, which could let malicious user obtain sensitive information. Patches available at: http://www.kernel.org/pub/linux/kernel/v2.6/patch-2.6.11.6.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel EXT2 File System Information Leak CAN-2005-0400	Medium	Security Focus, 12932, March 29, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0011, April 5, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 **RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005**
Multiple Vendors Linux kernel 2.6.10, 2.6, -test9-CVS, -test1-test11, 2.6.1-2.6.9; RedHat Desktop 4.0, Enterprise Linux WS 4, ES 4, AS 4	A Denial of Service vulnerability has been reported in the 'Unw_Unwind_To_User' function. RedHat; http://rhn.redhat.com/errata/RHSA-2005-366.html Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Unw_Unwind_To_User Denial of Service CAN-2005-0135	Low	RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005
Multiple Vendors Linux kernel 2.6.10, 2.6, -test9-CVS, -test1-test11, 2.6.1-2.6.9; RedHat Desktop 4.0, Enterprise Linux WS 4, ES 4, AS 4	A Denial of Service vulnerability has been reported in the 'fib_seq_start' function in 'fib_hash.c.' RedHat; http://rhn.redhat.com/errata/RHSA-2005-366.html Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 'Fib_Seq_Start' Denial of Service CAN-2005-1041	Low	RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005
Multiple Vendors Linux kernel 2.6-2.6.11	A vulnerability has been reported in 'SYS_EPoll_Wait' due to a failure to properly handle user-supplied size values, which could let a malicious user obtain elevated privileges. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html** An exploit script has been published.	Linux Kernel SYS_EPoll_Wait Elevated Privileges CAN-2005-0736	Medium	Security Focus, 12763, March 8, 2005 Ubuntu Security Notice, USN-95-1 March 15, 2005 Security Focus, 12763, March 22, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 **RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005**
Multiple Vendors Linux kernel 2.6-2.6.11	A vulnerability has been reported in the '/sys' file system due to a mismanagement of integer signedness, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code. SuSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntupool/main/l/linux-source-2.6.8.1/ **RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel SYSFS_Write_File Local Integer Overflow CAN-2005-0867	Low/ High (High if arbitrary code can be executed)	Security Focus, 13091, April 11, 2005 **RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005**

Multiple Vendors RedHat Fedora Core3, Core2; Rob Flynn Gaim 1.2; **Peachtree Linux release 1**	A remote Denial of Service vulnerability has been reported when an unspecified Jabber file transfer request is handled. Upgrade available at: http://gaim.sourceforge.net/downloads.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-05.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-365.html Mandrake: http://www.mandrakesecure.net/en/ftp.php **SGI:** **http://www.sgi.com/support/security/** **Peachtree:** **http://peachtree.burdell.org/updates/** There is no exploit code required.	Gaim Jabber File Request Remote Denial of Service CAN-2005-0967	Low	Fedora Update Notifications, FEDORA-2005-298 & 299, April 5, 2005 Gentoo Linux Security Advisory, GLSA 200504-05, April 06, 2005 RedHat Security Advisory, RHSA-2005:365-06, April 12, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:071, April 14, 2005 **SGI Security Advisory, 20050404-01-U, April 20, 2005** **Peachtree Linux Security Notice, PLSN-0001, April 21, 2005**
Multiple Vendors RedHat Fedora Core3, Core2; Rob Flynn Gaim 1.2; Ubuntu Linux 4.1 ppc, ia64, ia32; **Peachtree Linux release 1**	Two vulnerabilities have been reported: a remote Denial of Service vulnerability has been reported due to a buffer overflow in the 'gaim_markup_strip_html()' function; and a vulnerability has been reported in the IRC protocol plug-in due to insufficient sanitization of the 'irc_msg' data, which could let a remote malicious user execute arbitrary code. Update available at: http://gaim.sourceforge.net/downloads.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gaim/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-05.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-365.html Mandrake: http://www.mandrakesecure.net/en/ftp.php **SGI:** **http://www.sgi.com/support/security/** **Peachtree:** **http://peachtree.burdell.org/updates/** Currently we are not aware of any exploits for these vulnerabilities.	Gaim 'Gaim_Markup_Strip_HTML()' Function Remote Denial of Service & IRC Protocol Plug-in Arbitrary Code Execution CAN-2005-0965 CAN-2005-0966	Low/ High (High if arbitrary code can be executed)	Fedora Update Notifications, FEDORA-2005-298 & 299, April 5, 2005 Ubuntu Security Notice, USN-106-1 April 05, 2005 Gentoo Linux Security Advisory, GLSA 200504-05, April 06, 2005 RedHat Security Advisory, RHSA-2005:365-06, April 12, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:071, April 14, 2005 **SGI Security Advisory, 20050404-01-U, April 20, 2005** **Peachtree Linux Security Notice, PLSN-0001, April 21, 2005**
Multiple Vendors Samba 2.2.9, 3.0.8 and prior	An integer overflow vulnerability in all versions of Samba's smbd 0.8 could allow a remote malicious user to cause controllable heap corruption, leading to execution of arbitrary commands with root privileges. Patches available at: http://www.samba.org/samba/ftp/patches/security/samba-3.0.9-CAN-2004-1154.patch Red Hat: http://rhn.redhat.com/errata/	Multiple Vendors Samba smbd Security Descriptor CAN-2004-1154	High	iDEFENSE Security Advisory 12.16.04 Red Hat Advisory, RHSA-2004:670-10, December 16, 2004 Gentoo Security Advisory, GLSA 200412-13 / Samba, December 17, 2004 US-CERT, Vulnerability Note

	RHSA-2004-670.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-13.xml Trustix: http://www.trustix.net/errata/2004/0066/ Red Hat (Updated): http://rhn.redhat.com/errata/RHSA-2004-670.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: http://www.novell.com/linux/security/advisories/2004_45_samba.html Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:158 Conectiva: ftp://atualizacoes.conectiva.com.br/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-020.html HP: http://software.hp.com TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.17 **Debian:** **http://security.debian.org/pool/updates/main/s/samba/** Currently we are not aware of any exploits for this vulnerability.			VU#226184, December 17, 2004 Trustix Secure Linux Advisory #2004-0066, December 17, 2004 Red Hat, RHSA-2004:670-10, December 16, 2004 SUSE, SUSE-SA:2004:045, December 22, 2004 RedHat Security Advisory, RHSA-2005:020-04, January 5, 2005 Conectiva Linux Security Announcement, CLA-2005:913, January 6, 2005 Turbolinux Security Announcement, February 7, 2005 HP Security Advisory, HPSBUX01115, February 3, 2005 SCO Security Advisory, SCOSA-2005.17, March 7, 2005 Debian Security Advisory, DSA 701-1, March 31, 2005 **Debian Security Advisory, DSA 701-2, April 21, 2005**
Multiple Vendors xli 1.14-1.17	A vulnerability exists due to a failure to manage internal buffers securely, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200503-05.xml Debian: http://security.debian.org/pool/updates/main/x/xli/ ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for this vulnerability.	XLI Internal Buffer Management CAN-2005-0639	High	Gentoo Linux Security Advisory, GLSA 200503-05, March 2, 2005 Debian Security Advisory, DSA 695-1, March 21, 2005 ALTLinux Security Advisory, March 29, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:076, April 21, 2005**

Multiple Vendors xli 1.14-1.17; xloadimage 3.0, 4.0, 4.1	A vulnerability exists due to a failure to parse compressed images safely, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200503-05.xml Debian: http://security.debian.org/pool/updates/main/x/xli/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-332.html** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for this vulnerability.	XLoadImage Compressed Image Remote Command Execution CAN-2005-0638	High	Gentoo Linux Security Advisory, GLSA 200503-05, March 2, 2005 Fedora Update Notifications, FEDORA-2005-236 & 237, March 18, 2005 Debian Security Advisory, DSA 695-1, March 21, 2005 Turbolinux Security Advisory, TLSA-2005-43, April 19, 2005 **RedHat Security Advisory, RHSA-2005:332-10, April 19, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:076, April 21, 2005**
MySQL MySQL 4.x	A vulnerability exists in the 'mysqlaccess.sh' script because temporary files are created in an unsafe manner, which could let a malicious user obtain elevated privileges. Update available at: http://lists.mysql.com/internals/20600 Ubuntu: http://www.ubuntulinux.org/support/documentation/usn/usn-63-1 Debian: http://www.debian.org/security/2005/dsa-647 Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200501-33.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php FedoraLegacy: http://download.fedoralegacy.org/fedora/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** **OpenPKG:** **ftp://ftp.openpkg.org/release/2.2/UPD/mysql-4.0.21-2.2.2.src.rpm** Currently we are not aware of any exploits for this vulnerability.	MySQL 'mysqlaccess.sh' Unsafe Temporary Files CAN-2005-0004	Medium	Security Tracker Alert, 1012914, January 17,2005 Ubuntu Security Notice USN-63-1 January 18, 2005 Debian Security Advisory DSA-647-1 mysql, January 19, 2005 Gentoo GLSA 200501-33, January 23, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:036, February 11, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0003, February 11, 2005 Fedora Legacy Update Advisory, FLSA:2129, March 24, 2005 **Conectiva Linux Security Announcement, CLA-2005:947, April 20, 2005** **OpenPKG Security Advisory, OpenPKG-SA-2005.006, April 20, 2005**
openMosixview openMosixview 1.2-1.5	Multiple vulnerabilities have been reported due to the creation of various temporary files that contain predictable filenames, which could let a malicious user create/overwrite arbitrary files. **Gentoo:** **http://security.gentoo.org/glsa/glsa-200504-20.xml** A Proof of Concept exploit script has been published.	OpenMosixview Multiple Insecure Temporary File Creation CAN-2005-0894	Medium	Securiteam, March 28, 2005 **Gentoo Linux Security Advisory, GLSA 200504-20, April 21, 2005**

PHP Group PHP 4.3-4.3.10; **Peachtree Linux release 1**	A remote Denial of Service vulnerability has been reported when processing deeply nested EXIF IFD (Image File Directory) data. Upgrades available at: http://ca.php.net/get/php4.3.11.tar.gz/from/a/mirror Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-15.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php **Peachtree:** **http://peachtree.burdell.org/updates/** Currently, we are not aware of any exploits for this vulnerability.	PHP Group Exif Module IFD Nesting Remote Denial of Service CAN-2005-1043	Low	Security Focus, 13164, April 14, 2005 Ubuntu Security Notice, USN-112-1, April 14, 2005 Gentoo Linux Security Advisory, GLSA 200504-15, April 18, 2005 Fedora Update Notification, FEDORA-2005-315, April 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:072, April 19, 2005 **Peachtree Linux Security Notice, PLSN-0001, April 21, 2005**
PHP Group PHP 4.3-4.3.10; **Peachtree Linux release 1**	A vulnerability has been reported in the 'exif_process_IFD_TAG()' function when processing malformed IFD (Image File Directory) tags, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://ca.php.net/get/php4.3.11.tar.gz/from/a/mirror Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-15.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php **Peachtree:** **http://peachtree.burdell.org/updates/** Currently, we are not aware of any exploits for this vulnerability.	PHP Group Exif Module IFD Tag Integer Overflow CAN-2005-1042	High	Security Focus, 13163, April 14, 2005 Ubuntu Security Notice, USN-112-1, April 14, 2005 Gentoo Linux Security Advisory, GLSA 200504-15, April 18, 2005 Fedora Update Notification, FEDORA-2005-315, April 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:072, April 19, 2005 **Peachtree Linux Security Notice, PLSN-0001, April 21, 2005**

Remote Sensing LibTIFF 3.5.7, 3.6.1, 3.7.0; Avaya CVLAN, Integrated Management, Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0	Two vulnerabilities exist which can be exploited by malicious people to compromise a vulnerable system by executing arbitrary code. The vulnerabilities are caused due to an integer overflow in the "TIFFFetchStripThing()" function in "tif_dirread.c" when parsing TIFF files and"CheckMalloc()" function in "tif_dirread.c" and "tif_fax3.c" when handling data from a certain directory entry in the file header. Update to version 3.7.1: ftp://ftp.remotesensing.org/pub/libtiff/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://www.debian.org/security/2004/dsa-617 Gentoo: http://security.gentoo.org/glsa/glsa-200501-06.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-019.html SGI: http://support.sgi.com/browse_request/linux_patches_by_os TurboLinux: http://www.turbolinux.com/update/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-021_RHSA-2005-019.pdf Mandrake: http://www.mandrakesecure.net/en/ftp.php **Sun:** **http://sunsolve.sun.com/search/document.do?assetkey=1-26-57769-1** Currently we are not aware of any exploits for these vulnerabilities.	Remote Sensing LibTIFF Two Integer Overflow Vulnerabilities CAN-2004-1308	High	iDEFENSE Security Advisory 12.21.04 Secunia SA13629, December 23, 2004 SUSE Security Announcement, SUSE-SA:2005:001, January 10, 2005 RedHat Security Advisory, RHSA-2005:019-11, January 13, 2005 US-Cert Vulnerability Note, VU#125598, January 14, 2005 SGI Security Advisory, 20050101-01-U, January 19, 2005 Turbolinux Security Announcement, January 20, 2005 Conectiva Linux Security Announcement, CLA-2005:920, January 20, 2005 Avaya Security Advisory, ASA-2005-021, January 25, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:052, March 4, 2005 Sun(sm) Alert Notification, 57769, April 25, 2005
Roar Smith info2www 1.2.2.9	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Debian: http://security.debian.org/pool/updates/main/i/info2www/ There is no exploit code required.	Info2www Cross-Site Scripting CAN-2004-1341	High	Debian Security Advisory, DSA 711-1 , April 19, 2005

Rob Flynn Gaim 1.0-1.0.2, 1.1.1, 1.1.2	Multiple remote Denial of Service vulnerabilities have been reported when a remote malicious ICQ or AIM user submits certain malformed SNAC packets; and a vulnerability exists when parsing malformed HTML data. Upgrades available at: http://gaim.sourceforge.net/downloads.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gaim/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-03.xml Mandrake: Http://www.mandrakesecure.net/en/advisories/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-215.html Conectiva: ftp://atualizacoes.conectiva.com.br/ **Peachtree: http://peachtree.burdell.org/updates/** There is no exploit code required.	Gaim Multiple Remote Denials of Service CAN-2005-0472 CAN-2005-0473	Low	Gaim Advisory, February 17, 2005 Fedora Update Notifications, FEDORA-2005-159 & 160, February 21, 2005 US-CERT VU#839280 US-CERT VU#523888 Ubuntu Security Notice, USN-85-1 February 25, 2005 Gentoo Linux Security Advisory, GLSA 200503-03, March 1, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:049, March 4, 2005 RedHat Security Advisory, RHSA-2005:215-11, March 10, 2005 Conectiva Linux Security Announcement, CLA-2005:933, March 14, 2005 **Peachtree Linux Security Notice, PLSN-0002, April 21, 2005**
SWSoft Confixx Pro 3, Confixx 3.0.6, 3.0.8	An SQL injection vulnerability has been reported due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	SWSoft Confixx SQL Injection CAN-2005-1302	High	Security Focus, 13355, April 25, 2005
Vladislav Bogdanov SNMP Proxy Daemon 0.4-0.4.5	A format string vulnerability has been reported in SNMPPD due to insufficient sanitization of user-supplied input before using in a formatted printing function, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	SNMPPD SNMP Proxy Daemon Remote Format String CAN-2005-1246	High	INetCop Security Advisory #2005-0x82-027, April 24, 2005

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Albrecht Guenther PHProjekt 4.2 & prior	A Cross-Site Scripting vulnerability has been reported in the chatroom text submission form due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	PHProjekt Chat Script Cross-Site Scripting CAN-2005-1227	High	Secure Science Corporation Application Software Advisory 055, April 20, 2005
AZ Bulletin Board AZbb 1.0.7 a-1.0.7 c	Multiple vulnerabilities have been reported: a vulnerability was reported in 'admin_avatar.php' and 'admin_attachment.php' due to validation errors, which could let a remote malicious user with administrative privileges delete arbitrary files; a vulnerability was reported in 'main_index.php' due to insufficient verification of input passed to the 'dir_src' and 'abs_layer' parameters, which could let a remote malicious user include arbitrary files; and a Directory Traversal vulnerability has been reported in 'attachment.php' due to an input validation error, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://azbb.cyaccess.com/azbb.php?1091872271 There is no exploit code required.	AZ Bulletin Board Multiple Vulnerabilities CAN-2005-1200 CAN-2005-1201	Medium	GulfTech Security Research , April 19, 2005

bBlog bBlog 0.7.4	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability has been reported due to insufficient validation of the entry title field or comment body text, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability has been reported in the 'postid' parameter, which could let a remote malicious user execute arbitrary SQL commands. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	bBlog 'postid' Cross-Site Scripting & SQL Injection CAN-2005-1309 CAN-2005-1310	High	Security Tracker Alert, 1013811, April 26, 2005
Castlehill	A Directory Traversal vulnerability has been reported in the third party tool from Castlehill, as used to secure the iSeries AS/400 FTP server, which could lead to a false sense of security. Contact the vendor for details regarding obtaining and applying appropriate updates. There is no exploit code required.	Castlehill Directory Traversal CAN-2005-1240	Medium	Bugtraq, 396628, April 20, 2005
DUware DUportal 3.1.2 SQL, 3.1.2	Multiple SQL injection vulnerabilities have been reported due to insufficient sanitization of user-supplied input before using in SQL queries, which could let a remote malicious user execute arbitrary SQL code. *Note: This this is a different set of vulnerabilities than the other DUportal Pro issue.* No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	DUportal Multiple SQL Injection CAN-2005-1236	High	Dcrab 's Security Advisory, April 20, 2005
DUware DUportal Pro 3.4	Multiple SQL injection vulnerabilities have been reported due to insufficient sanitization of user-supplied input before using in SQL queries, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	DUportal Pro Multiple SQL Injection CAN-2005-1224	High	Dcrab 's Security Advisory, April 20, 2005
eGroupWare eGroupWare 1.0-1.0.3, 1.0.6	Multiple unspecified vulnerabilities have been fixed in the latest upgrade. The impact was not specified. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=78745 **Gentoo: http://security.gentoo.org/glsa/glsa-200504-24.xml** Currently we are not aware of any exploits for these vulnerabilities.	eGroupWare Multiple Vulnerabilities CAN-2005-1202 CAN-2005-1203	Not Specified	Security Focus, 13212, April 18, 2005 **Gentoo Linux Security Advisory, GLSA 200504-24, April 25, 2005**
Ethereal Group Ethereal 0.8, 0.8.13-0.8.15, 0.8.18, 0.8.19, 0.9-0.9.16, 0.10-0.10.9	A remote Denial of Service vulnerability has been reported due to the way Resource ReSerVation Protocol (RSVP) packets are decoded. No workaround or patch available at time of publishing. An exploit script has been published.	Ethereal RSVP Decoding Routines Denial of Service CAN-2005-1281	Low	Security Focus, 13391, April 26, 2005
FlexPHPNews FlexPHPNews .3	An SQL injection vulnerability was reported in 'news.php' due to insufficient sanitization of the 'newsid' parameter, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	FlexPHPNews News.PHP SQL Injection CAN-2005-1237	High	Secunia Advisory, SA14905, April 21, 2005
Fritz Berger yappa-ng 0.9, 1.0-1.6, 2.0 .0, 2.0.1, 2.1.0-2.3.1	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of certain unspecified input, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability has been reported due to insufficient verification of unspecified input before using to include files, which could let a remote malicious user include arbitrary files from external and local resources. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=70802 There is no exploit code required.	Yappa-NG Cross-Site Scripting & File Include CAN-2005-1311 CAN-2005-1312	High	Secunia Advisory, SA15107, April 26, 2005
GNU Gaim prior to 1.1.4	A vulnerability exists in the processing of HTML that could let a remote malicious user crash the Gaim client. This is due to a NULL pointer dereference. Update to version 1.1.4: http://gaim.sourceforge.net/downloads.php	GNU Gaim Denial of Service Vulnerability CAN-2005-0208	Low	Sourceforge.net Gaim Vulnerability Note, February 24, 2005 US-CERT VU#795812 Gentoo, GLSA 200503-03, March 1, 2005

	Ubuntu: http://www.ubuntulinux.org/support/documentation/usn/usn-85-1 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-03.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-215.html Conectiva: ftp://atualizacoes.conectiva.com.br/ **Peachtree:** **http://peachtree.burdell.org/updates/** Currently we are not aware of any exploits for this vulnerability.			Mandrakelinux Security Update Advisory, MDKSA-2005:049, March 4, 2005 RedHat Security Advisory, RHSA-2005:215-11, March 10, 2005 Conectiva Linux Security Announcement, CLA-2005:933, March 14, 2005 **Peachtree Linux Security Notice, PLSN-0002, April 21, 2005**
Gregory DEMAR Coppermine Photo Gallery 1.0 RC3, 1.1 beta 2, 1.1 .0, 1.2, 1.2.1, 1.2.2 b, 1.3	A vulnerability has been reported in the 'include/init.inc.php' script due to insufficient sanitization of user-supplied input before written in log files, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/coppermine/cpg1.3.3.zip?download There is no exploit code required.	Coppermine Photo Gallery 'include/init.inc.php' HTML Injection CAN-2005-1172	High	Bugtraq, 396080, April 18, 2005 **Security Focus, 13218, April 20, 2005**
Gregory DEMAR Coppermine Photo Gallery 1.3.2	Multiple vulnerabilities have been reported: An SQL injection vulnerability was reported in Favs due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; An SQL injection vulnerability was reported in 'ZipDownload.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported because passwords are stored in plaintext in the database, which could let a remote malicious user obtain sensitive information. Upgrade available at: http://prdownloads.sourceforge.net/coppermine/cpg1.3.3.zip?download Currently we are not aware of any exploits for these vulnerabilities.	Coppermine Photo Gallery Multiple Vulnerabilities CAN-2005-1225 CAN-2005-1226	Medium/ High (High if arbitrary SQL code can be executed)	waraxe-2005-SA#042 Advisory, April 20, 2005
Horde Project Horde Passwd Module 2.x	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.horde.org/passwd/download/ There is no exploit code required.	Horde Passwd Module Parent Frame Page Title Cross-Site Scripting CAN-2005-1313	High	Secunia Advisory, SA15075, April 25, 2005
Horde Project Horde Kronolith Module	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.horde.org/kronolith/download/ There is no exploit code required.	Horde Kronolith Module Parent Frame Page Title Cross-Site Scripting CAN-2005-1314	High	Secunia Advisory, SA15080, April 25, 2005
Horde Project HordeTurba Module 1.x	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.horde.org/turba/	Horde Turba Module Parent Frame Page Title Cross-Site Scripting	High	Secunia Advisory, SA15074, April 25, 2005

	download/ There is no exploit code required.	CAN-2005-1315		
Horde Project Horde Accounts Module 2.1, 2.1.1	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.horde.org/accounts/download/ There is no exploit code required.	Horde Accounts Module Parent Frame Page Title Cross-Site Scripting CAN-2005-1316	High	Secunia Advisory, SA15081, April 25, 2005
Horde Project Horde Chora 1.1-1.2.2	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.horde.org/chora/download/ There is no exploit code required.	Horde Chora Parent Frame Page Title Cross-Site Scripting CAN-2005-1317	High	Secunia Advisory, SA15083, April 25, 2005
Horde Project Horde Forwards Module 2.1-2.2.1	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.horde.org/forwards/download/ There is no exploit code required.	Horde Forwards Module Parent Frame Page Title Cross-Site Scripting CAN-2005-1318	High	Secunia Advisory, SA15082, April 25, 2005
Horde Project Horde IMP Webmail Client 3.x	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: ftp://ftp.horde.org/pub/imp/imp-3.2.8.tar.gz There is no exploit code required.	Horde IMP Webmail Client Parent Frame Page Title Cross-Site Scripting CAN-2005-1319	High	Secunia Advisory, SA15080, April 25, 2005
Horde Project Horde Mnemo 1.1-1.1.3	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.horde.org/mnemo/download/ There is no exploit code required.	Horde Mnemo Parent Frame Page Title Cross-Site Scripting CAN-2005-1320	High	Secunia Advisory, SA15078, April 25, 2005
Horde Project Horde Vacation 2.0-2.2.1	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.horde.org/vacation/download/ There is no exploit code required.	Horde Vacation Parent Frame Page Title Cross-Site Scripting CAN-2005-1321	High	Secunia Advisory, SA15073, April 25, 2005
Horde Project HordeNag 1.1-1.1.2	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.horde.org/nag/download/ There is no exploit code required.	Horde Nag Parent Frame Page Title Cross-Site Scripting CAN-2005-1322	High	Secunia Advisory, SA15079, April 25, 2005
IBM Websphere Application Server 6.0	A Cross-Site Scripting vulnerability has been reported due to an error when the requested filename is included in the 404 HTTP error message, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	IBM WebSphere Application Server Error Page Cross-Site Scripting	High	Secunia Advisory, SA15067, April 25, 2005
IBM iSeries AS400	A Directory Traversal vulnerability has been reported in the AS400 FTP Service, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	IBM iSeries AS400 FTP Service Directory Traversal CAN-2005-1238	Medium	Security Focus, 13298, April 21, 2005

InterSoft NetTerm .1.1	A buffer overflow vulnerability has been reported in the USER command when an overly long string is submitted, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. An exploit script has been published.	Intersoft NetTerm USER Remote Buffer Overflow CAN-2005-1323	High	Security Focus, 13396, April 26, 2005
Invision Power Services Invision Board 2.0.1	An SQL injection vulnerability was reported due to insufficient sanitization of the 'QPid' parameter, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Invision Power Board 'QPid' Parameter SQL Injection	High	Security Focus, 13375, April 26, 2005
MediaWiki MediaWiki 1.x	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of certain unspecified input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/wikipedia/mediawiki-1.4.2.tar.gz?download There is no exploit code required.	MediaWiki Cross-Site Scripting CAN-2005-1245	High	Secunia Advisory, SA14993, April 21, 2005
Mozilla.org Mozilla Browser 1.0-1.0.2, 1.1-1.7.6, Firefox 0.8-0.10.1, 1.0.1, 1.0.2	Multiple vulnerabilities have been reported: a vulnerability was reported in the 'EMBED' tag for non-installed plugins when processing the 'PLUGINSPAGE' attribute due to an input validation error, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because blocked popups that are opened through the GUI incorrectly run with 'chrome' privileges, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because the global scope of a window or tab are not cleaned properly before navigating to a new web site, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because the URL of a 'favicons' icon for a web site isn't verified before changed via JavaScript, which could let a remote malicious user execute arbitrary code with elevated privileges; a vulnerability was reported because the search plugin action URL is not properly verified before used to perform a search, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to the way links are opened in a sidebar when using the '_search' target, which could let a remote malicious user execute arbitrary code; several input validation vulnerabilities were reported when handling invalid type parameters passed to 'InstallTrigger' and 'XPInstall' related objects, which could let a remote malicious user execute arbitrary code; and vulnerabilities were reported due to insufficient validation of DOM nodes in certain privileged UI code, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.mozilla.org/products/firefox/ http://www.mozilla.org/products/mozilla1.x/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-18.xml **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-383.html** **http://rhn.redhat.com/errata/RHSA-2005-386.html** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** There is no exploit code required.	Mozilla Suite / Firefox Multiple Vulnerabilities CAN-2005-0752 CAN-2005-1153 CAN-2005-1154 CAN-2005-1155 CAN-2005-1156 CAN-2005-1157 CAN-2005-1158 CAN-2005-1159 CAN-2005-1160	High	Mozilla Foundation Security Advisories, 2005-35 - 2005-41, April 16, 2005 Gentoo Linux Security Advisory, GLSA 200504-18, April 19, 2005 US-CERT VU#973309 **RedHat Security Advisories, RHSA-2005:383-07 & RHSA-2005-386., April 21 & 26, 2005** **Turbolinux Security Advisory, TLSA-2005-49, April 21, 2005** **US-CERT VU#519317**

Multiple Vendors Mozilla.org Mozilla Browser 1.7.6, Firefox 1.0.1, 1.0.2; K-Meleon K-Meleon 0.9; Netscape 7.2; K-Meleon 0.9	A vulnerability has been reported in the javascript implementation due to improper parsing of lamba list regular expressions, which could a remote malicious user obtain sensitive information. The vendor has issued a fix, available via CVS. **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-383.html** **http://rhn.redhat.com/errata/RHSA-2005-386.html** **Slackware:** **http://www.mozilla.org/projects/security/known-vulnerabilities.html** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** There is no exploit code required; however, a Proof of Concept exploit has been published.	Mozilla Suite/Firefox JavaScript Lambda Information Disclosure CAN-2005-0989	Medium	Security Tracker Alert, 1013635, April 4, 2005 Security Focus, 12988, April 16, 2005 **RedHat Security Advisories, RHSA-2005:383-07 & RHSA-2005:386-08, April 21 & 26, 2005** **Turbolinux Security Advisory, TLSA-2005-49, April 21, 2005** **Slackware Security Advisory, SSA:2005-111-04, April 22, 2005**
Multiple Vendors MPlayer 1.0pre6 & prior; Xine 0.9.9-1.0; Peachtree Linux release 1	Several vulnerabilities have been reported: a buffer overflow vulnerability has been reported due to a boundary error when processing lines from RealMedia RTSP streams, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability has been reported due to a boundary error when processing stream IDs from Microsoft Media Services MMST streams, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.mplayerhq.hu/MPlayer/patches/rtsp_fix_20050415.diff Gentoo: http://security.gentoo.org/glsa/glsa-200504-19.xml Patches available at: http://cvs.sourceforge.net/viewcvs.py/xine/xinelib/src/input/ Currently we are not aware of any exploits for these vulnerabilities.	MPlayer RTSP & MMST Streams Buffer Overflow CAN-2005-1195	High	Security Tracker Alert,1013771, April 20, 2005 Gentoo Linux Security Advisory, GLSA 200504-19, April 20, 200 Peachtree Linux Security Notice, PLSN-0003, April 21, 2005 Xine Security Announcement, XSA-2004-8, April 21, 2005
Multiple Vendors See US-CERT VU#222750 for complete list	Multiple vendor implementations of TCP/IP Internet Control Message Protocol (ICMP) do not adequately validate ICMP error messages, which could let a remote malicious user cause a Denial of Service. Cisco: http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml IBM: ftp://aix.software.ibm.com/aix/efixes/security/icmp_efix.tar.Z RedHat: http://rhn.redhat.com/errata/ Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendor TCP/IP Implementation ICMP Remote Denial of Service CAN-2004-1060 CAN-2004-0790 CAN-2004-0791	Low	**US-CERT VU#222750**
MySQL AB MaxDB 7.5 .00.23-7.5.00.25, 7.5 .00.19, 7.5 .00.18, 7.5 .00.14-7.5 .00.16, 7.5 .00.12, 7.5 .00.11, 7.5 .00.08, 7.5 .00	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported due to a boundary error in the web administration service when a specially crafted long HTTP 'GET' request is submitted that contains a percent sign, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability was reported in 'WDVHandler_CommonUtils.c' due to a boundary error in the 'getLockTokenHeader()' function, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://dev.mysql.com/downloads/maxdb/7.5.00.html Currently we are not aware of any exploits for these vulnerabilities.	MySQL MaxDB Remote Buffer Overflows CAN-2005-0684 CAN-2005-1274	High	Secunia Advisory, SA15109, April 26, 2005

MySQL AB MySQL 4.0.23, and 4.1.10 and prior	A vulnerability was reported in the CREATE FUNCTION command that could let an authenticated user gain mysql user privileges on the target system and permit the user to execute arbitrary code. A fixed version (4.0.24 and 4.1.10a) is available at: http://dev.mysql.com/downloads/index.html Gentoo: http://security.gentoo.org/glsa/glsa-200503-19.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ ALT Linux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-334.html SuSE: ftp://ftp.suse.com/pub/suse/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/m/mysql/ **OpenPKG:** **ftp://ftp.openpkg.org/release/2.2/UPD/mysql-4.0.21-2.2.2.src.rpm** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** A Proof of Concept exploit has been published.	MySQL CREATE FUNCTION Remote Code Execution Vulnerability CAN-2005-0709	High	Security Tracker Alert ID: 1013415, March 11, 2005 Gentoo Linux Security Advisory, GLSA 200503-19, March 16, 2005 Ubuntu Security Notice, USN-96-1 March 16, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:060, March 21, 2005 Trustix Secure Linux Security Advisory, TSL-2005-0009, March 21, 2005 SUSE Security Announcement, SUSE-SA:2005:019, March 24, 2005 RedHat Security Advisory, RHSA-2005:334-07, March 28, 2005 ALTLinux Security Advisory, March 29, 2005 Conectiva Linux Security Announcement, CLA-2005:946, April 4, 2005 Debian Security Advisory, DSA 707-1 , April 13, 2005 **OpenPKG Security Advisory, OpenPKG-SA-2005.006, April 20, 2005** **Turbolinux Security Advisor, TLSA-2005-48, April 21, 2005**
NetIQ Corporation NetIQ	A Directory Traversal vulnerability has been reported in the third party tool from NetIQ, as used to secure the iSeries AS/400 FTP server, which could lead to a false sense of security. No workaround or patch available at time of publishing. There is no exploit code required	NetIQ Directory Traversal CAN-2005-1244	Medium	Bugtraq, 396628, April 20, 2005
Netref Netref 4.2	A vulnerability has been reported in the 'script/cat_for_gen.php' script due to insufficient validation of the 'ad_direct' and 'm_for_racine' parameters, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Netref 'Cat_for_gen.PHP' Remote PHP Script Injection CAN-2005-1222	High	Secunia Advisory, SA15040, April 20, 2005
North American Systems International BSafe	A Directory Traversal vulnerability has been reported in the third party tool from Bsafe, as used to secure the iSeries AS/400 FTP server, which could lead to a false sense of security. No workaround or patch available at time of publishing. There is no exploit code required.	Bsafe Directory Traversal CAN-2005-1242	Medium	Bugtraq, 396628, April 20, 2005
Oracle Corporation Oracle Application Server 10g, Enterprise Edition, Personal Edition, Standard Edition	Multiple SQL injection vulnerabilities have been reported due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary SQL code. **An SQL injection vulnerability was reported in the 'SYS.DBMS_CDC_IPUBLISH.CREATE_SCN_CHANGE_SET' standard procedure, which could let a remote malicious user execute arbitrary SQL code; An SQL injection vulnerability was reported in 'ALTER_MANUALLOG_**	Oracle Database Multiple SQL Injection	High	Security Focus 13144, April 12, 2005 US-CERT VU#982109 **AppSecInc Team SHATTER Security Advisories, April 18,**

	CHANGE_SOURCE' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code; and An SQL injection vulnerability was reported in the 'SUBSCRIPTION_NAME' parameter due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary SQL code. Update information available at: http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf Proofs of Concept exploits have been published.			**2005**
Oracle Corporation Oracle Application Server 10g, Enterprise Edition, Personal Edition, Standard Edition, Oracle9i Enterprise, Edition 8.1.7, 9.0.1.5, 9.0.1 .4, 9.0.1, 9.0.4, 9.2 .0-9.2.0.6, Oracle9i Lite 5.0 .2.9.0, 5.0.2.0.0, 5.0 .1.0.0, 5.0 .0.0.0 Oracle9i Personal Edition 8.1.7, 9.0.1.5, 9.0.1 .4, 9.0.1, 9.0.4, 9.2 .0-9.2.0.6, 9.2, Oracle9i Standard Edition 8.1.7, 9.0, 9.0.1-9.0.1 .5, 9.0.2, 9.0.4, 9.2 .3, 9.2.0.1-9.2.0.6, 9.2	Several vulnerabilities have been reported: An SQL injection vulnerability was reported in the 'OBJECT_TYPE' parameter that is used by the 'DBMS_METADATA' package due to insufficient sanitization, which could let a remote malicious user execute arbitrary SQL code; and a remote Denial of Service vulnerability has been reported due to insufficient sanitization of user-supplied input. Update information available at: http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf Proofs of Concept exploits have been published.	Oracle Database SQL Injection & Denial of Service	Low / High (High if arbitrary code can be executed)	Security Focus, 13238 & 13239, April 18, 2005 US-CERT VU#982109
Palace Guard Software Secure/NET+	An input validation vulnerability has been reported due to a failure to filter potentially dangerous character sequences from user requests, which could lead to a false sense of security. Contact the vendor for details regarding obtaining and applying appropriate updates. There is no exploit code required.	Palace Guard Software Secure/NET+ Input Validation	Medium	Bugtraq, 396628, April 20, 2005
PHP Group PHP prior to 5.0.4; **Peachtree Linux release 1**	Multiple Denial of Service vulnerabilities have been reported in 'getimagesize().' Upgrade available at: http://ca.php.net/get/php-4.3.11.tar.gz/from/a/mirror Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Slackware: ftp://ftp.slackware.com/pub/slackware/ Debian: http://security.debian.org/pool/updates/main/p/php3/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Gentoo: http://security.gentoo.org/glsa/glsa-200504-15.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **Peachtree:** **http://peachtree.burdell.org/updates/** Currently we are not aware of any exploits for these vulnerabilities.	PHP 'getimagesize()' Multiple Denials of Service CAN-2005-0524 CAN-2005-0525	Low	iDEFENSE Security Advisory, March 31, 2005 Ubuntu Security Notice, USN-105-1, April 05, 2005 Slackware Security Advisory, SSA:2005-095-01, April 6, 2005 Debian Security Advisory, DSA 708-1, April 15, 2005 SUSE Security Announcement, SUSE-SA:2005:023, April 15, 2005 Gentoo Linux Security Advisory, GLSA 200504-15, April 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:072, April 19, 2005 **Peachtree Linux Security Notice, PLSN-0001, April 21, 2005**
PHP Labs proFile	A Cross-Site Scripting vulnerability has been reported in the 'index.php' script due to insufficient validation of the 'dir' and 'file' parameters, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	PHP Labs proFile Cross-Site Scripting CAN-2005-1233	High	sNKenjoi's Security Advisory, April 18, 2005

phpBB Group phpBB 2.0-2.0.14	Cross-Site Scripting vulnerabilities have been reported in the 'profile.php,' and 'viewtopic.php' scripts due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPBB Cross-Site Scripting CAN-2005-1290	High	[N]eo [S]ecurity [T]eam [NST]® - Advisory #14, April 17, 2005
phpbb-auction phpbb-auction 1.0, 1.2	Two vulnerabilities have been reported: a vulnerability was reported in 'auction_rating.php' due to insufficient sanitization of the 'u' parameter and in 'action_offer.php' due to insufficient sanitization of the 'ar' parameter, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability has been reported in 'auction_myauctions.php' in the 'mode' parameter, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	PHPBB-Auction SQL Injection & Information Disclosure CAN-2005-1234 CAN-2005-1235	Medium/ High (High if arbitrary SQL code can be executed)	sNKenjoi's Security Advisory, ZH2005-12SA, April 20, 2005
phpMyVisites phpMyVisites 1.0-1.3	A Cross-Site Scripting vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'part,' 'per,' and 'site' parameters, which could let a remote malicious user execute arbitrary HTML and script code. Patches available at: http://cvs.sourceforge.net/cvstarballs/phpmyvisites-cvsroot.tar.bz2 There is no exploit code required.	PHPMyVisites Cross-Site Scripting CAN-2005-1324	High	Secunia Advisory, SA15084, April 25, 2005
phpMyVisites phpMyVisites 1.3	A vulnerability has been reported in the 'Set_Lang' file variable, which could let a malicious user obtain sensitive information. Patches available at: http://cvs.sourceforge.net/cvstarballs/phpmyvisites-cvsroot.tar.bz2 A Proof of Concept exploit has been published.	PHPMyVisites Set_Lang File Include CAN-2005-1325	Medium	Security Focus, 13370, April 26, 2005
PixySoft E-Cart 1.1	A vulnerability has been reported in the'index.cgi' script due to insufficient validation of the 'cat' and 'art' variables, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	PixySoft E-Cart Input Validation CAN-2005-1289	High	Security Tracker Alert, 1013780, April 21, 2005
PowerTech PowerLock	A Directory Traversal vulnerability has been reported in the third party tool from Powertech, as used to secure the iSeries AS/400 FTP server, which could lead to a false sense of security. Contact the vendor for details regarding obtaining and applying appropriate updates. There is no exploit code required.	PowerTech PowerLock Directory Traversal CAN-2005-1241	Medium	Bugtraq, 396628, April 20, 2005
profitCode Software PayProCart 3.0	Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization input passed to the 'username,' 'chckoutaction,' 'ckprvd,' 'pageID,' 'hdoc,' 'modID,' 'taskID,' 'proMod,' and 'mmactionComm' parameters, which could let a remote malicious user execute arbitrary HTML and script code; It is also possible to disclose the full path to certain scripts by accessing them directly. Upgrade available at: http://www.profitcode.net/products/payprocart-31.html There is no exploit code required; however, Proofs of Concept exploits have been published.	ProfitCode Software PayProCart Multiple Cross-Site Scripting & Path Disclosure	Medium/ High (High if arbitrary code can be executed)	Secunia Advisory, SA15025, April 21, 2005
Python SimpleXMLRPCServer 2.2 all versions, 2.3 prior to 2.3.5, 2.4	A vulnerability exists in the SimpleXMLRPCServer library module that could permit a remote malicious user to access internal module data, potentially executing arbitrary code. Python XML-RPC servers that use the register_instance() method to register an object without a _dispatch() method are affected. Patches for Python 2.2, 2.3, and 2.4, available at: http://python.org/security/PSF-2005-001/patch-2.2.txt (Python 2.2) http://python.org/security/PSF-2005-001/patch.txt	Python SimpleXMLRPC Server Remote Code CAN-2005-0088 CAN-2005-0089	High	Python Security Advisory: PSF-2005-001, February 3, 2005 Gentoo, GLSA 200502-09, February 08, 2005 Mandrakesoft, MDKSA-2005:035, February 10, 2005 Trustix #2005-0003,

	(Python 2.3, 2.4) The vendor plans to issue fixed versions for 2.3.5, 2.4.1, 2.3.5, and 2.4.1. Debian: http://www.debian.org/security/2005/dsa-666 Gentoo: http://security.gentoo.org/glsa/glsa-200502-09.xml Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:035 Trustix: http://www.trustix.org/errata/2005/0003/ Red Hat: http://rhn.redhat.com/errata/RHSA-2005-109.html SUSE: ftp://ftp.SUSE.com/pub/SUSE Debian: http://security.debian.org/pool/updates/main/liba/libapache-mod-python/ **Slackware:** **ftp://ftp.slackware.com/pub/slackware/** Currently we are not aware of any exploits for this vulnerability.			February 11, 2005 RedHat Security Advisory, RHSA-2005:109-04, February 14, 2005 SUSE Security Summary Report, SUSE-SR:2005:005, February 18, 2005 US-CERT VU#356409 Debian Security Advisory, DSA 689-1, February 23, 2005 **Slackware Security Advisory, SSA:2005-111-02, April 22, 2005**
Raz-Lee Security+++ Suite	A Directory Traversal vulnerability has been reported in the third party tool from Raz-Lee, as used to secure the iSeries AS/400 FTP server, which could lead to a false sense of security. Contact the vendor for details regarding obtaining and applying appropriate updates. There is no exploit code required.	Raz-Lee Security+++ Suite Directory Traversal CAN-2005-1239	Medium	Bugtraq, 396628, April 20, 2005
SafeStone Technologies SafeStone	A Directory Traversal vulnerability has been reported in the third party tool from SafeStone, as used to secure the iSeries AS/400 FTP server, which could lead to a false sense of security. No workaround or patch available at time of publishing. There is no exploit code required	SafeStone Directory Traversal CAN-2005-1243	Medium	Bugtraq, 396628, April 20, 2005
Sun Microsystems, Inc. OpenOffice 1.1.4, 2.0 Beta	A vulnerability has been reported due to a heap overflow when a specially crafted malformed '.doc' file is opened, which could lead to a Denial of Service or execution of arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-13.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-375.html** Currently we are not aware of any exploits for this vulnerability.	OpenOffice Malformed Document Remote Heap Overflow CAN-2005-0941	Low/ High (High if arbitrary code can be executed)	Security Focus, 13092, April 11, 2005 Fedora Update Notification, FEDORA-2005-316, April 13, 2005 Gentoo Linux Security Advisory, GLSA 200504-13, April 15, 2005 SUSE Security Announcement, SUSE-SA:2005:025, April 19, 2005 **RedHat Security Advisory, RHSA-2005:375-07, April 25, 2005**
Sun Microsystems, Inc. Sun Java Web Proxy Server 3.6, SP1-SP6	Multiple buffer overflow vulnerabilities have been reported due to an unspecified error, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.sun.com/download/products.xml?id=424217a1 Currently we are not aware of any exploits for these vulnerabilities.	Sun Java System Web Proxy Server Multiple Remote Buffer Overflows CAN-2005-1232	High	Sun(sm) Alert Notification, 57763 , April 19, 2005

UBBCentral UBB.threads 6.0	An SQL injection vulnerability has been reported in the 'Printthread.php' script due to insufficient sanitization of the 'main' parameter, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	UBBCentral UBB.threads 'Printthread.PHP' SQL Injection CAN-2005-1199	High	Secunia Advisory, SA15024, April 20, 2005
University of California (BSD License) PostgreSQL 7.x, 8.x; **Peachtree Linux release 1**	Multiple vulnerabilities exist that could permit malicious users to gain escalated privileges or execute arbitrary code. These vulnerabilities are due to an error in the 'LOAD' option, a missing permissions check, an error in 'contrib/intagg,' and a boundary error in the plpgsql cursor declaration. Update to version 8.0.1, 7.4.7, 7.3.9, or 7.2.7: http://wwwmaster.postgresql.org/download/mirrors-ftp Ubuntu: http://www.ubuntulinux.org/support/documentation/usn/usn-71-1 Debian: http://www.debian.org/security/2005/dsa-668 Gentoo: http://security.gentoo.org/glsa/glsa-200502-08.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/postgresql/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-141.html Gentoo: http://security.gentoo.org/glsa/glsa-200502-19.xml Debian: http://security.debian.org/pool/updates/main/p/postgresql/ Mandrakesoft: http://www.mandrakesoft.com/security/ advisories?name=MDKSA-2005:040 **SUSE: ftp://ftp.SUSE.com/pub/SUSE** **Peachtree: http://peachtree.burdell.org/updates/** **Trustix: http://www.trustix.org/errata/2005/0015/** Currently we are not aware of any exploits for these vulnerabilities.	University of California PostgreSQL Multiple Vulnerabilities CAN-2005-0227 CAN-2005-0246 CAN-2005-0244 CAN-2005-0245 CAN-2005-0247	Medium/ High (High if arbitrary code can be executed)	PostgreSQL Security Release, February 1, 2005 Ubuntu Security Notice USN-71-1 February 01, 2005 Debian Security Advisory DSA-668-1, February 4, 2005 Gentoo GLSA 200502-08, February 7, 2005 Fedora Update Notifications, FEDORA-2005-124 & 125, February 7, 2005 Ubuntu Security Notice,e USN-79-1 , February 10, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0003, February 11, 2005 Gentoo Linux Security Advisory, GLSA 200502-19, February 14, 2005 RedHat Security Advisory, RHSA-2005:141-06, February 14, 2005 Debian Security Advisory, DSA 683-1, February 15, 2005 Mandrakesoft, MDKSA-2005:040, February 17, 2005 SUSE Security Summary Report, SUSE-SR:2005:005, February 18, 2005 Fedora Update Notifications, FEDORA-2005-157 &158, February 22, 2005 SUSE Security Summary Report, SUSE-SR:2005:006, February 25, 2005 **SUSE Security Announcement, SUSE-SA:2005:027, April 20, 2005** **Peachtree Linux Security Notice, PLSN-0004, April 21, 2005** **Trustix Secure Linux Security Advisory, TSLSA-2005-0015, April 25, 2005**

VooDoo cIRCle 1.0.20, 1.0.32	A remote Denial of Service vulnerability has been reported when handling packets from BOTNET connections due to a boundary error. Upgrades available at: http://prdownloads.sourceforge.net/voodoo-circle/voodoo_circle-doc-1.0.33.zip?download Currently we are not aware of any exploits for this vulnerability.	VooDoo Circle BotNet Connection Remote Denial of Service CAN-2005-1326	Low	Secunia Advisory: SA15110, April 26, 2005
WebCT WebCT Campus Edition 4.1	A vulnerability has been reported due to insufficient sanitization of user-supplied input before used in dynamically generated content, which could let a remote malicious user execute arbitrary HTML and script code. **Workaround available at: http://www.webct.com/support/viewpage?name=support_bulletins#apr15-05** There is no exploit code required; however, a Proof of Concept exploit has been published.	WebCT Discussion Board Arbitrary Code Execution CAN-2005-1076	High	Security Focus, 13101, April 11, 2005 **Security Focus, 13101, April 22, 2005**
Woltlab Burning Board 2.3.1	A Cross-Site Scripting vulnerability has been reported in the 'pms.php' script due to insufficient validation, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	WoltLab Burning Board 'PMS.PHP' Cross-Site Scripting CAN-2005-1327	High	Security Focus, 13353, April 25, 2005
Woltlab Burning Board 2.3.1	A Cross-Site Scripting vulnerability has been reported in the 'thread.php' script due to insufficient validation of the 'hilight' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	WoltLab Burning Board 'Thread.PHP' Cross-Site Scripting CAN-2005-1285	High	Security Tracker Alert, 1013790, April 23, 2005

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
April 26, 2005	7330ecart.pl	No	Proof of Concept exploit for the PixySoft E-Cart Input Validation vulnerability.
April 26, 2005	exp_netftpd.py	No	Script that exploits the Intersoft NetTerm USER Remote Buffer Overflow vulnerability.
April 26, 2005	xtcpdump+ethr-rsvp-dos.c	No	Script that exploits the Ethereal RSVP Decoding Routines Denial of Service vulnerability.
April 26, 2005	xtcpdump-bgp-dos.c xtcpdump-isis-dos.c xtcpdump-ldp-dos.c xtcpdump+ethr-rsvp-dos.c	No	Scripts that exploit the TCPDump BGP Decoding Routines Denial Of Service vulnerability.
April 25, 2005	ophcrack-2.0.tar.gz	N/A	A cracker aimed at NT-style (LANMAN) password-hashes that uses a large precomputed hash database to crack the majority of all passwords within a matter of seconds.
April 25, 2005	x0n3-h4ck_mailenable_https.pl	No	Perl script that exploits the MailEnable HTTP Authorization Buffer Overflow vulnerability.
April 21, 2005	kill-bill.tar.gz msasn1_ms04_007_killbill.pm	Yes	Proofs of Concept exploits for the Microsoft Windows ASN.1 Library Bit String Processing Variant Heap Corruption vulnerability.
April 20, 2005	DMA_2005-0412a_.txt	No	Exploit for the WIDCOMM Bluetooth Connectivity Software is Directory Traversal vulnerability.
April 20, 2005	HLLUBBThreadsExploit.c	No	Proof of Concept exploit for the UBBCentral UBB.threads 'Printthread.PHP' SQL Injection vulnerability
April 20, 2005	MS05-021-PoC.pl	Yes	Proof of Concept exploit for the Microsoft Exchange Server Remote Code Execution Vulnerability.

April 20, 2005	pmSoftwareSimpleWebBufferOverflowPoC.pl pmSoftwareSimpleWebOverflowExploit.c pmx.c	No	Scripts that exploit the PMSoftware Simple Web Server Buffer Overflow Permits Remote Code Execution vulnerability
April 20, 2005	predebug1.c predebug2.c	N/A	Example predebug code execution exploit, demonstrating how programmers being loaded into debuggers can attack the machine running the debugger.
April 19,2005	wheresjames.c	No	Proof of Concept exploit for the WheresJames Webcam Publisher Web Server Buffer Overflow vulnerability.
April 19, 2005	copy.doc simple.doc rename.doc	No	Scripts that exploit the Microsoft Windows Explorer Preview Pane Script Injection vulnerability
April 19, 2005	ie_dhtml_poc.txt	Yes	Proof-of-Concept exploit for the MSIE DHTML object handling vulnerabilities.
April 19, 2005	MSHTA_POC.c	Yes	Proof-of-Concept exploit that generates a file with an embedded CLSID.
April 19, 2005	msjet40.txt	Yes	Microsoft Jet exploit that makes use of an insufficient data validation vulnerability.
April 19, 2005	oracle_sdo_code_size.c	Yes	Exploit for the Oracle Database 'MDSYS.MD2.SDO_CODE_SIZE' Buffer Overflow vulnerability.
April 19, 2005	plsql_multiplestatement_injection.txt	N/A	Specialized exploit for cases where SQL injection is possible against a Oracle PL/SQL setup.
April 18, 2005	EXPL-A-2005-006.txt	No	Example exploit URLs for the XAMPP Remote HTML Injection & Password Disclosure vulnerability.
April 18, 2005	gg_crack.c	N/A	Utility that decrypts stored passwords for the "Gadu-Gadu" Polish-language chat program.
April 18, 2005	PreDebug.pdf	N/A	A whitepaper that describes how malicious code can be forced to run when a binary is loaded into a debugger / disassembler for analysis.

[back to top]

Trends

- **Phishing attacks catch sensitive human resources information:** Experts have warned that organized crime gangs are developing sophisticated 'phishing' attacks against businesses to try to steal passwords and sensitive information. Businesses are being targeted because the rewards are greater. Source: http://www.personneltoday.com/Articles/2005/04/22/29400/Phishing+attacks+catch+sensitive+HR+information.htm.
- **Trojan horses take aim at Symbian cell phones:** According to a cell phone antivirus software company, SimWorks, 52 new Trojan horses are hidden inside several different cell phone games and other mobile phone software. These Trojans contain malicious software that crashes many critical cell phone components that use Symbian. Source: http://news.com.com/Trojan+horses+take+aim+at+Symbian+cell+phones/2100-7349_3-5678211.html.
- **Cyber attack early warning center begins pilot project:** The Cyber Incident Detection Data Analysis Center (CIDDAC), backed by a grant from the U.S. Department of Homeland Security, has set up an operations center at the University of Pennsylvania's Institute of Strategic Threat Analysis and Response laboratory. They are beginning a pilot project to collect data on network intrusions from a group of companies in national-infrastructure industries .Source: http://www.infoworld.com/article/05/04/20/HNcyberpilot_1.html.
- **Virus writers turning from e-mail to IM**: Email worms are falling out of favor with the hacking community, according to a report investigating malicious internet activity. Instead malware authors are increasingly subverting vulnerable instant messenger (IM) systems and using network viruses that do not require user interaction to spread. Other threats identified include botnets and increasingly intrusive adware. The study identifies 40 individual IM worms in the first quarter of the year, the majority written in one of the simplest computer languages, Visual Basic (VB). It noted that use of this language indicates the authors are relatively unsophisticated coders, since VB is not widely used by experts because it is so slow to run. Report: http://www.viruslist.com/en/analysis?pubid=162454316 Source: http://www.vnunet.com/news/1162557
- **Unpatched machines seen as major security threat**: Hackers will keep developing exploits that take advantage of known software vulnerabilities because, although patches are available, a minority of machines are fixed, security vendor McAfee said Monday, April 25. AVERT Report: http://www.mcafeesecurity.com/us/about/press/corporate/2005/20050425_185320.htm Source: http://www.informationweek.com/story/showArticle.jhtml;jsessionid=ZWPITNXHXNCIMQSNDBCSKH0CJUMEKJVN?articleID=161502434

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Netsky-Q	Win32 Worm	Stable	March 2004

3	Zafi-D	Win32 Worm	Stable	December 2004
4	Mytob.C	Win32 Worm	Stable	March 2004
5	Bagle.BJ	Win32 Worm	Stable	January 2005
6	Netsky-D	Win32 Worm	Stable	March 2004
6	Netsky-Z	Win32 Worm	Stable	April 2004
7	Zafi-B	Win32 Worm	Stable	June 2004
7	Netsky-B	Win32 Worm	Stable	February 2004
8	Bagle-AU	Win32 Worm	Stable	October 2004
8	Sober-I	Win32 Worm	Stable	November 2004

Table Updated April 26, 2005

Viruses or Trojans Considered to be a High Level of Threat

- None to report.

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Backdoor.Ripgof		Trojan
Backdoor.Ryejet.B		Trojan
Bagle.CM	W32/Bagle.CM.worm	Win32 Worm
Haxdoor	Backdoor.Win32.Haxdoor	Trojan
Lecna	Backdoor.Win32.Lecna.b	Trojan
Mitglieder.CG	Trj/Mitglieder.CG	Trojan
Mytob.BD	Net-Worm.Win32.Mytob.m W32/Mytob.BD.worm	Win32 Worm
PWS-Banker.gen.d		Trojan
PWSteal.Bancos.T		Trojan
SYMBOS_SKULLS.I	SymbOS.Skulls.D SymbOS.Skulls.H	
Troj/CashGrab-A	Trojan.Win32.Agent.cw PWS-Cashgrabber TROJ_AGENT.DLA	Trojan
Troj/CashGrab-B	Trojan-Dropper.Win32.Agent.hp Trojan.Win32.Agent.cc	Trojan
Troj/Dloader-MK	Trojan-Downloader.Win32.Agent.bq Downloader-YN TROJ_DLOADER.HD	Trojan
Troj/Dloader-MN	Downloader-YS	Trojan
Troj/Kelvir-P		Trojan
Troj/Kelvir-R	IM-Worm.Win32.Prex.d	Trojan
Trojan.Abwiz		Trojan
Trojan.Admincash.B		Trojan
Trojan.Aiminfo		Trojan
Trojan.Drivus	Exploit-1Table Trojan-Dropper.MSWord.1Table.a	Trojan
Trojan.Flush.C	Trojan.Win32.DNSChanger.a	Trojan
Trojan.Goldun.E		Trojan
Trojan.Horrortel	Trojan-Dropper.Win32.Delf.ji Trojan.News	Trojan
Trojan.Horrortel.B		Trojan
Trojan.Nephtebank		Trojan
Trojan.Riler.B		Trojan
Trojan.Riler.C		Trojan
Trojan.Servpam		Trojan
Trojan.Yabinder		Trojan
Trojan.Zhopa		Trojan
W32.Ahker.G@mm		Win32 Worm
W32.Beagle.BP@mm		Win32 Worm
W32.Gabloliz.A		Win32 Worm
W32.Kedebe@mm		Win32 Worm

W32.Kelvir.AE		Win32 Worm
W32.Kelvir.AF	Trojan-IM.Win32.Prex.a	Win32 Worm
W32.Kelvir.AH		Win32 Worm
W32.Kelvir.AI	W32/Kelvir.worm.gen	Win32 Worm
W32.Kelvir.AJ	IM-Worm.Win32.Prex.d W32/Bropia.worm.ag	Win32 Worm
W32.Kelvir.AL		Win32 Worm
W32.Kelvir.AO		Win32 Worm
W32.Mytob.BE@mm	Net-Worm.Win32.Mytob.gen W32/Mytob.gen@MM	Win32 Worm
W32.Mytob.BJ@mm	Net-Worm.Win32.Mytob.am W32/Mytob.gen@MM	Win32 Worm
W32.Mytob.BL@mm	Net-Worm.Win32.Mytob.gen	Win32 Worm
W32.Mytob.BM@mm	Net-Worm.Win32.Mytob.af W32/Mytob.gen@MM WORM_MYTOB.CA	Win32 Worm
W32.Mytob.BN@mm	Net-Worm.Win32.Mytob.gen W32/Mydoom.gen@MM	Win32 Worm
W32.Mytob.BO@mm	Net-Worm.Win32.Mytob.x	Win32 Worm
W32.Sober.N@mm!dr		Win32 Worm
W32.Spybot.OBB		Win32 Worm
W32.Spybot.OBZ		Win32 Worm
W32.Velkbot.A	Backdoor.Win32.SdBot.gen W32/Sdbot.worm.gen.j	Win32 Worm
W32/Antiman-A	Email-Worm.Win32.Antiman.a	Win32 Worm
W32/LegMir-AD	Trojan.Win32.VB.kj TROJ_LEGMIR.B	Win32 Worm
W32/Mytob-AG	Net-Worm.Win32.Mytob.af WORM_MYTOB.CA	Win32 Worm
W32/Mytob-AH		Win32 Worm
W32/Mytob-AI		Win32 Worm
W32/Mytob-AJ		Win32 Worm
W32/Mytob-AK	WORM_MYTOB.BT	Win32 Worm
W32/Nopir-B		Win32 Worm
W32/Rbot-AAY		Win32 Worm
W32/Rbot-ABB		Win32 Worm
W32/Sdbot-ZC		Win32 Worm
W32/Sober-M		Win32 Worm
W32/Wurmark-I	Email-Worm.Win32.Wurmark.i	Win32 Worm
Win32.Bagle.BG		Win32 Worm
Win32.Chisyne.F		Win32 Worm
Win32.Codalush		Win32 Worm
Win32.Glieder.AC		Win32 Worm
Win32.Glieder.AF		Win32 Worm
Win32.Kelvir.L	W32/Kelvir-L	Win32 Worm
Win32.Kelvir.N		Win32 Worm
Win32.WinAd.G		Win32 Worm
Win32/Antiman.A@mm	W32.Antiman.A@mm W32/Antiman.A@mm W32/Generic.Delphi WORM_ANTIMAN.A	Win32 Worm
WORM_ANTIMAN.B		Win32 Worm
WORM_BAGLE.BI	Email-Worm.Win32.Bagle.bj W32.Beagle.BO@mm W32/Bagle Win32.Bagle.BI	Win32 Worm
WORM_KEBEDE.B		Win32 Worm
WORM_KEDEBE.A	W32.Kedebe@mm	Win32 Worm
WORM_KELVIR.AA	W32.Kelvir.AB W32/Kelvir.Q	Win32 Worm
WORM_KELVIR.AB	IM-Worm.Win32.Kelvir.y W32.Kelvir.AN W32/Generic.worm!p2p W32/GenericP2P.worm WORM_KELVIR.AD	Win32 Worm
WORM_KELVIR.X	W32.Kelvir.AE	Win32 Worm
WORM_KELVIR.Y	W32.Kelvir.AF	Win32 Worm

WORM_KELVIR.Z	W32.Kelvir	Win32 Worm
WORM_MYTOB.BV		Win32 Worm
WORM_MYTOB.CA	W32.Mytob.AH@mm	Win32 Worm
WORM_MYTOB.CB	Mytob.BC Net-Worm.Win32.Mytob.t W32/Mytob.BC.worm	Win32 Worm
WORM_MYTOB.CC	Net-Worm.Win32.Mytob.gen W32.Mytob.BC@mm W32/Mytob.BZ@mm W32/Mytob.gen@MM	Win32 Worm
WORM_MYTOB.CD	Net-Worm.Win32.Mytob.gen W32.Mytob.BD@mm W32/Mytob.gen@MM	Win32 Worm
WORM_MYTOB.CH	Net-Worm.Win32.Mytob.gen W32.Mytob.BH@mm W32/Mytob.CC@mm W32/Mytob.gen@MM Win32/Mytob.S@mm	Win32 Worm
WORM_MYTOB.CI	W32.Randex.gen W32/Mytob.CB@mm	Win32 Worm
WORM_MYTOB.CJ	W32/Mytob	Win32 Worm
WORM_MYTOB.CK	W32.Mytob.AF@mm	Win32 Worm
WORM_MYTOB.CL	W32.Mytob.AH@mm	Win32 Worm
WORM_MYTOB.CM		Win32 Worm
WORM_MYTOB.CN		Win32 Worm
WORM_MYTOB.CU	W32.Mytob.BE@mm W32/Mytob W32/Mytob.CE@mm Win32/Mytob.AN@mm	Win32 Worm
WORM_MYTOB.CY		Win32 Worm

[back to top]

Last updated April 28, 2005